IDENTITEETTITIETOISEN VERKKOARKKITEHTUURIN KÄYTTÖÖNOTON TESTAUS KANTA-HÄMEEN SAIRAANHOITOPIIRISSÄ

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Ammattikorkeakoulun opinnäytetyö

Tietotekniikan koulutusohjelma

Riihimäen yksikkö kevät 2013

Sensuroitu versio

Timo Tupala

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Riihimäki
Tietotekniikka
Tietoliikennetekniikka

TIIVISTELMÄ

Tekijä Timo Tupala **Vuosi** 2013

Työn nimi Identiteettitietoisen verkkoarkkitehtuurin käyttöönoton testaus Kanta-Hämeen Sairaanhoitopiirissä (Sensuroitu versio)

TIIVISTELMÄ

Tietoverkkojen käyttäjämäärät sekä verkkolaitteiden määrät ovat hurjassa kasvussa. Kanta-Hämeen Keskussairaalan kokoisessa laitoksessa verkkoa käyttävien ihmisten ja laitteiden määrä on päivittäin tuhansissa. Jotta verkon käyttö pysyisi tietoturvallisena ei toimintaa voida jatkaa entisellään.

Tässä opinnäytetyössä keskitytään Cisco Systemsin ratkaisuun hallita suurien käyttäjä- ja päätelaitemäärien pääsyä verkkoon hallitusti ja tietoturvallisesti. Opinnäytetyössä asennetaan KHSHP:n verkkoon Identity Services Engine joka hoitaa dynaamista 802.1X pääsynhallintaa, sertifikaattipalvelut, sekä Prime-järjestelmä verkkolaitteiden keskitettyä hallintaa varten. Tavoitteena on testata kuinka helposti tämä ratkaisu olisi otettavissa tuotantokäyttöön ja olisiko ratkaisu tarkoituksenmukainen.

Työn teoriaosuudessa keskitytään IEEE 802.1X standardiin sekä siinä käytettyihin erilaisiin protokolliin kuten EAP ja RADIUS. Työssä esitellään myös mitä identiteettitietoinen verkkoarkkitehtuuri on, sekä ne Ciscon ohjelmistot ja laitteistot joita työssä tullaan käyttämään.

Työssä ISE:lle konfiguroitiin halutut autentikointi ja autorisointi politiikat ja identiteettilähteet. 802.1X tunnistautumismenetelmiä testattiin käyttöjärjestelmillä Windows XP ja Windows 7. Molempien käyttöjärjestelmien omien supplikanttien lisäksi Ciscon Anyconnectin toimivuus testattiin läpikotaisin. ISE:llä käytettiin niin sanottua ”Monitor Modea” jolloin testaus voitiin suorittaa käyttäjiä häiritsemättä. Prime-järjestelmä käytiin läpi pintapuolisemmin, mutta toimivuus saatiin testattua ja todettua hyväksi.

Työn tuloksena saatiin vahvaa näyttöä ISE:n toimivuudesta sairaalaympäristössä. Supplikantit saatiin konfiguroitua onnistuneesti ja konfiguraatiot ovat valmiita jaeltavaksi kaikille koneille. Työ dokumentoitiin ISE:n mahdollista tuotantokäyttöä varten selkeäksi ohjeeksi.

Avainsanat Tietoliikenne, pääsynvalvonta, lähiverkot, langattomat lähiverkot, IEEE 802.1X

Sivut 66 s. + liitteet 7 s.

HAMK
UNIVERSITY OF APPLIED SCIENCES

ABSTRACT

Riihimäki
Information technology
Telecommunications technology

Author Timo Tupala **Year** 2013

Subject of Bachelor's thesis Testing of identity aware network architechture's deployment in Kanta-Häme Central Hospital (Sensured version)

ABSTRACT

Amount of users and devices in networks are rising rapidly. In department size of Kanta-Häme Central Hospital, there are thousands of invidual users and devices utilizing our network every day. To gurantee a safe network usage to everyone we can't continue operating like we are doing now.

In this thesis we concentrate in Cisco Systems' solution to handle access control and safety for large volume of network clients. During this thesis we deploy Identity Services Engine to the hospital network that manages dynamic 802.1X access control, install certificate server and setup Prime Infrastructure for centralized managing of network devices. Objective is to test how easy or not it would be to harness this solution into production network and would it be functional for our needs.

In the theory part of this thesis we focus on IEEE 802.1X standard and it's protocols like EAP and RADIUS. Thesis also introduces what identity aware network architechture is and all the software and hardware we use to create it.

During the thesis project we configured different authentication and authorization politics and identity sources into Cisco ISE. 802.1X authentication methods were tested on Windows XP and Windows 7. In addition to native supplicants of both operating systems, we tested Cisco's Anyconnect supplicant thoroughly. So called "Monitor Mode" was used in ISE to test all the configurations and politics without disturbing any of the clients. Testing of Prime Infrastructure was more or less perfunctory, but still, it's functionality was proven to be of great worth.

As a result for this thesis we got vast amount of hard evidence that talks in behalf of ISE and its positive functionality in hospital network environment. All the supplicants were successfully configured and those configurations are ready to be deployed to the workstations. Thesis was also documented as a guide for future deployment of ISE in hospital environment.

Keywords Telecommunication, access control, LAN, WLAN, IEEE 802.1
Pages 66 p. + appendices 7 p.

SISÄLLYS

1 JOHDANTO 1

2 TYÖN LÄHTÖKOHDAT 1

2.1 Työn toimeksiantaja 1
2.2 Työn tavoitteet 2

3 NYKYINEN VERKKOARKKITEHTUURI 2

3.1 Yleistä 2
3.2 Hallinnolliset ja operatiiviset haasteet 3
3.3 Tietoturvariskit nykyisellä verkkoarkkitehtuurilla 4
3.3.1 LAN–verkon tietoturvariskit 4
3.3.2 WLAN–verkon tietoturvariskit 4
3.4 Raportoitavuus ja näkyvyys 4

4 IEEE 802.1X STANDARDI 5

4.1 Yleistä standardista 5
4.1.1 Supplikantti 6
4.1.2 Autentikaattori 6
4.1.3 Autentikointipalvelin 7
4.2 EAP 7
4.2.1 EAP-paketin koostumus 8
4.2.2 EAP-pakettityypit 9
4.3 EAPoL-protokolla 10
4.3.1 EAPoL kapselointi 11
4.3.2 EAPoL-paketin koostumus 11
4.3.3 EAPoL-pakettityypit 12
4.4 RADIUS-protokolla 14
4.4.1 RADIUS-paketin koostumus 15
4.4.2 RADIUS-paketin tyypit 17
4.5 EAP-Methods-protokolla 19
4.5.1 EAP-Method -paketin koostumus 20

5 IDENTITEETTITIETOINEN VERKKOARKKITEHTUURI 21

5.1 Mitä on identiteettitietoinen verkkoarkkitehtuuri 21
5.2 Hyödyt verrattuna nykyiseen verkkoarkkitehtuuriin 22
5.3 Haasteet uudella identiteettitietoisella verkkoarkkitehtuurilla 22
5.4 Ratkaisuksi Cisco TrustSec 22
5.4.1 Cisco Identity Services Engine (ISE) 23
5.4.2 Cisco Prime 24
5.4.3 Cisco Anyconnect 25

6 TOTEUTUS 26

6.1 Yleistä 26
6.2 Käytössä olevat ja testattavat tunnistautumismenetelmät 26
6.2.1 Testattavat 802.1X-tunnistautumismenetelmät 26
6.2.2 MAC Authentication Bypass eli MAB 27

6.2.3 WEB-tunnistautuminen 28
6.3 Sertifikaattipalvelin ja PK-Infrastruktuuri 28
6.4 Identiteettilähteet 29
6.5 Identity Service Enginen pystytys 30
6.6 Wireless Lan Controllerin liittäminen Identity Services Engineen 30
6.7 Kytkinten eli autentikaattoreiden konfigurointi 31
6.8 Identity Services Enginen konfigurointi 31
6.8.1 Autentikaattorien lisääminen Identity Services Engineen 31
6.8.2 Identiteettilähteiden konfigurointi 32
6.8.3 Autentikonti politiikka 33
6.8.4 Autorisointi profiilit 34
6.8.5 Autorisointi politiikka 34

7 SUPPLIKANTTIEN KONFIGUROINTI JA TESTAUS 35

7.1 Windows XP 35
7.1.1 Win XP LAN 802.1X EAP-PEAP Microsoftin supplikantilla 38
7.1.2 Win XP WLAN 802.1X EAP-PEAP Microsoftin supplikantilla 40
7.1.3 Win XP LAN 802.1X EAP-TLS Microsoftin supplikantilla 40
7.1.4 Win XP WLAN 802.1X EAP-TLS Microsoftin supplikantilla 41
7.2 Windows 7 42
7.2.1 Windows 7 LAN 802.1X EAP-PEAP Microsoftin supplikantilla 43
7.2.2 Windows 7 WLAN 802.1X EAP-PEAP Microsoftin supplikantilla 44
7.2.3 Windows 7 LAN 802.1X EAP-TLS Microsoftin supplikantille 45
7.2.4 Windows 7 WLAN 802.1X EAP-TLS Microsoftin supplikantilla 46
7.3 Cisco Anyconnect konfigurointi 47
7.3.1 Client Policy 48
7.3.2 Authentication Policy 48
7.3.3 Networks 49
7.3.4 Network Groups 50
7.3.5 Network Profile KHSHP-LAN 51
7.3.6 Network Profile KHSHP-WLAN 54
7.4 Cisco Anyconnect testaus 55
7.4.1 Win XP LAN 802.1X EAP-PEAP Ciscon Anyconnectilla 57
7.4.2 Win XP LAN 802.1X EAP-TLS Ciscon Anyconnectilla 57
7.4.3 Win XP WLAN 802.1X EAP-PEAP Ciscon Anyconnectilla 57
7.4.4 Win XP WLAN 802.1X EAP-TLS Ciscon Anyconnectilla 57
7.4.5 Windows 7 LAN 802.1X EAP-PEAP Ciscon Anyconnectilla 58
7.4.6 Windows 7 LAN 802.1X EAP-TLS Ciscon Anyconnectilla 58
7.4.7 Windows 7 WLAN 802.1X EAP-PEAP Ciscon Anyconnectilla 58
7.4.8 Windows 7 WLAN 802.1X EAP-TLS Ciscon Anyconnectilla 58
7.5 Mac Authentication Bypass testaus 58

8 RAPORTOINTI JA VIANSELVITYS 59

8.1 ISE Raportointi ja vianselvitys 59
8.2 Prime raportointi ja vianselvitys 59

9 JOHTOPÄÄTÖKSET 61

LÄHTEET 63

LIITTEET 64

LYHENTEET

AAA	Authentication, Authorization and Accounting. Autentikointi, valtuutus ja tilastointi.
ACS	Secure Access Control Server. Ciscon pääsynhallinta palvelin.
AD	Active Directory. Microsoftin versio LDAP-hakemistopalvelusta.
ASA	Access Service Appliance. Ciscon palomuuriratkaisu.
CA	Certificate Authority. Digitaalisten sertifikaattien myöntäjä.
DHCP	Dynamic Host Configuration Protocol. Verkkoprotokolla jonka avulla verkkolaitteille tarjoillaan ip osoitteet.
DNS	Domain Name System. Nimipalvelujärjestelmä jolla IP:t muunnetaan verkkotunnuksiksi.
EAP	Extensive Authentication Protocol. Todennusprotokollan runko jonka avulla tunnistetietoja välitetään.
EAPoL	Extensive Authentication Protocol over LAN. Tekniikka, jolla EAP-viestejä kuljetetaan lähiverkoissa.
EAP-TLS	Extensive Authentication Protocol – Tarnsport Layer Security. Salausprotokolla, joka käyttää sertifikaatteja tietoliikenteen suojaukseen.
GPO	Group Policy Object. Ryhmäkäytäntöobjekti, sisältää toimipaikkoja, toimialueita ja organisaatioyksikköjä koskevat ryhmäkäytäntöasetukset.
IEEE	Institute of Electrical and Electronics Engineers. Tekniikan alan kansaivälinen järjestö joka määrittelee ja julkaisee alan standardeja.
ICMP	Internet Control Message Protocol. TCP/IP-pinon kontrolliprotokolla.
IP	Internet Protocol. TCP/IP-mallin Internet-kerroksen protokolla, joka huolehtii IP-tietoliikennepakettien toimittamisesta perille.

ISE	Identity Services Engine. Ciscon järjestelmä, joka hallinnoi identiteettitietoista pääsynhallintaa verkossa.
LAN	Local Area Network. Rajoitetulla maantieteellisellä alueella toimiva tietoliikenneverkko.
MAB	MAC Address Bypass. Tekniikka ISE:ssä, jolla voidaan MAC-osoitteen avulla ohittaa 802.1X-autentikointi.
MAC	Media Access Control. Verkkosovittimen ethernet-verkossa yksilöivä osoite.
MS-CHAPv2	Microsoft Challenge-Handshake Authentication Protocol. Microsoftin versio CHAP-protokollasta. Mahdollistaa kaksisuuntaisen todentamisen.
PEAP	Protected Extensive Authentication Protocol. Todennusprotokolla, jossa sertifikaatti sijaitsee vain todentavalla palvelimella.
SSH	Secure Shell. Salattuun tietoliikenteeseen tarkoitettu protokolla.
SSID	Service Set Identifier. Langattoman lähiverkon verkkotunnus.
VLAN	Virtual Local Area Network. Virtuaalinen lähiverkko.
WLC	Wireless Lan Controller. Cisco Systemsin langattoman verkon kontrolleri.
WLAN	Wireless Local Area Network. Langaton lähiverkko.

1 JOHDANTO

Lähiverkkoon liittyvien laitteiden ja käyttäjien määrän lisääntyessä, myös tunnistusmenetelmien ja pääsynhallinnan tulee kehittyä. Opinnäytetyön aihe valikoituikin juuri tämän tarpeen tullessa esille Kanta-Hämeen Sairaahoitopiirissä. Aihe sopii todella hyvin koulutussuuntaani sekä työnkuvaan tietoliikennetekniikan parissa. Cisco Systemsin esittelemä identiteettipohjaisuuteen perustuva järjestelmä tuntuu juuri sopivalle ratkaisulle KHSHP:n kokoisessa laitoksessa. KHSHP:lle tekemässäni insinöörityössä keskitytään tämän järjestelmän käyttöönoton mahdollisuuksiin ja sen tarkoituksenmukaisuuden kartoittamiseen sekä samalla toimivan ohjeen luontiin tulevaisuutta varten.

Tavoitteena on saada asennettua ja testattua sairaalassa käytössä olevaan IT- ja verkkoinfrastruktuuriin Ciscon tarjoama Identity Services Engine. Tarkoituksena on testata ja määrittää millaisia ponnisteluja vaatisi tämän järjestelmän käyttöönotto koko tuotantoverkon laajuisesti ilman, että joudutaan tekemään suuria taloudellisia investointeja. Testaus aiotaankin suorittaa suoraan sairaalan tuotantoverkossa, jotta saadaan mahdollisimman autenttinen kuva oikean käyttöönoton mahdollisista ongelmista. Työn aikana on tarkoitus testata myös Ciscon Prime-järjestelmä, jolla pystytään valvomaan verkon aktiivilaitteita keskitetysti.

Työn aikana pystyn pureutumaan syvemmin koulussa oppimiini asioihin Cisco Systemsin laitteiden konfiguroinneista sekä verkkojen tietoturvasta. Voin käyttää kaikkea opinnäytetyössäni oppimaa suoraa omassa ammatissani sairaalan verkkojen ylläpitäjänä. Opinnäytetyöstä on tarkoitus tehdä sellainen, että sitä voidaan käyttää suoraa oppaana, jos ISE:n pohjalle rakennettu pääsynhallintaratkaisu otetaan sairaalalla tuotantokäyttöön. Supplikanttien ja palvelinten konfigurointi pyritään dokumentoimaan mahdollisimman tarkasti ja selkeästi.

Työssä tullaan käyttämään läpi teoriaa suojatusta ja identiteettipohjaisesta pääsynhallinnasta, identiteettilähteistä, sertifikaattipalveluista sekä erilaisista työssä käytetyistä tietoliikenne- ja suojausprotokollista.

2 TYÖN LÄHTÖKOHDAT

2.1 Työn toimeksiantaja

Työn toimeksiantajana toimii Kanta-Hämeen Keskussairaala. Kanta-Hämeen sairaanhoitopiirin kuntayhtymään kuuluu 11 jäsenkuntaa, joiden asukasmäärä on noin 175 000. Kuntayhtymän palveluksessa on noin 2 000 henkilöä. Kanta-Hämeen Keskussairaalan Hämeenlinnan yksikkö palvelee kaikkia sairaanhoitopiirin asukkaita ja Riihimäen yksikkö ensisijaisesti Riihimäen seudun kuntien asukkaita eli yhteensä noin 62 400 asukasta. Vuonna 2012 yksittäisiä poliklinikkakäyntejä kirjattiin yli 210 000 ja hoitopäiviä reilut 105 000. (KHSHP Suoriteraportti 3b 2012)

2.2 Työn tavoitteet

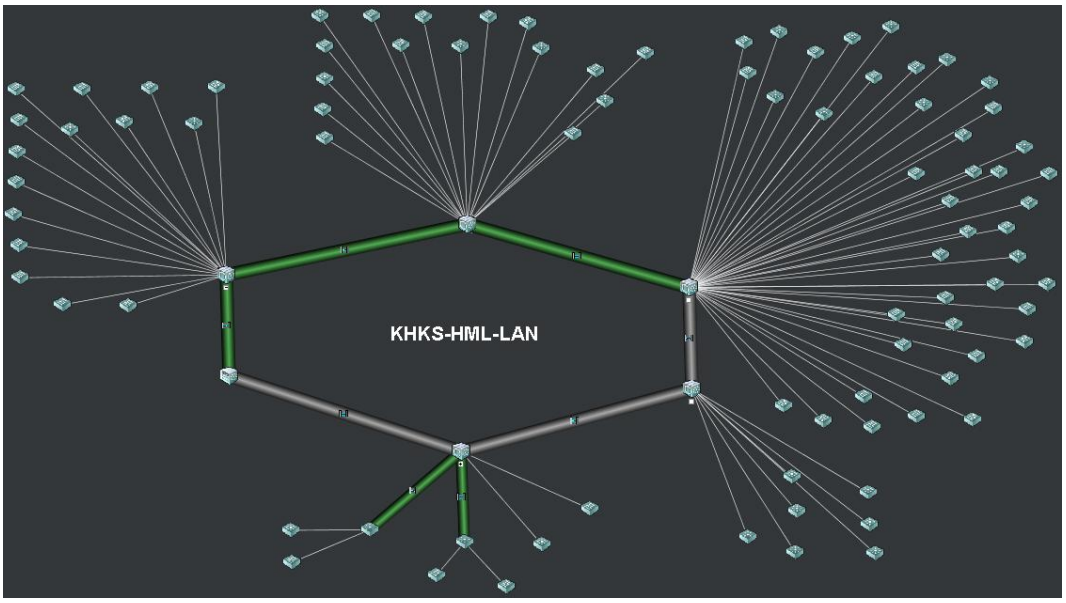
Opinnäytetyön tavoitteena on testata ja arvioida identiteettitietoisen verkkoarkkitehtuurin käyttöönoton mahdollisuuksia Kanta-Hämeen Sairaanhoitopiirin Hämeenlinnan ja Riihimäen yksiköissä. Arkkitehtuuri tullaan rakentamaan Ciscon Systemsin laitteiden päälle, joihin nykyinenkin verkkoinfrastruktuuri perustuu. Päätavoitteina on saada tarpeeksi informaatiota aiheesta, jotta voidaan tehdä päätös onko mahdollista ja kannattaako sairaalan ottaa käyttöön 802.1X arkkitehtuuri Ciscon Identity Service Enginellä. Käyttöönoton perusteina olisivat sekä langattoman, että langallisen verkon tietoturvan parantaminen, raportoinnin ja näkyvyyden kehittäminen sekä kustannustehokkaamman toiminnan edistäminen.

3 NYKYINEN VERKKOARKKITEHTUURI

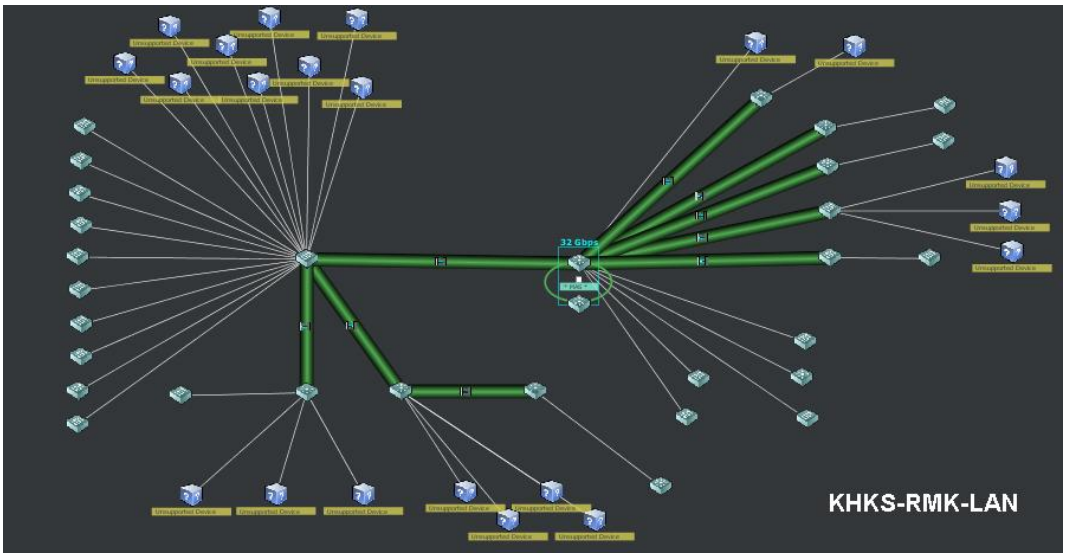
3.1 Yleistä

Kanta-Hämeen Keskussairaalan tietoliikenneverkko koostuu lähes kokonaan Cisco Systemsin valmistamista kytkimistä ja reitittimistä, sekä langattomista tukiasemista. Käytössä olevia kytkinmalleja ovat Catalyst 2950, 2960, 2960S ja 4500 sekä tukiasemat Ciscon AIR-LAP1142N-E-K9 ja AIR-AP1231G-E-K9-mallia. Topologiaan on liitettynä myös Ciscon Secure Access Control System (ACS) jolla tällä hetkellä hoidetaan lähinnä client VPN-yhteyksiä, Wireless Lan Controller (WLC) langattoman verkon keskitettyä hallintaa varten sekä palomuurina Ciscon kahdennettu ASA 5500. Kytkimiä on verkkoon liitettynä noin 170 kappaletta ja tukiasemia noin 100 kappaletta. Tukiasemat saavan konfiguraatiot ja ohjelmistopäivityksensä keskitetysti kontrollerilta, mutta kytkimien tilanne ei ole aivan yhtä hyvä. Nykyisellä kokoonpanolla jokainen kytkin ja jokainen portti on konfiguroitava manuaalisesti muutosten yhteydessä. Keskimäärin tästä muodostuu 8000 manuaalisesti määriteltävää kohdetta. Samasta syystä johtuen IOS-ohjelmistoversiotkaan eivät ole kaikissa kytkimissä yhteneväiset.

Fyysiset runkolinjat on rakennettu yhdistelmänä OS1-yksimuotokuitua, OM3- ja GKL-monimuotokuitua sekä CAT5a-, CAT6- ja CAT6a-kuparijohtimia. Itse reitittävien kytkinten välinen runkoyhteys muodostuu kahdennetusta 10Gbit OS1–yksimuotokuidusta.



Kuva 1. KHSHP Hämeenlinnan yksikön verkkotopologia.



Kuva 2. KHSHP Riihimäen yksikön verkkotopologia.

3.2 Hallinnolliset ja operatiiviset haasteet

Selkeimmät hallinnolliset ja operatiiviset haasteet nykyisellä verkkoarkkitehtuurilla muodostuvat kytkinten suuren määrän myötä koituvasta työtaakasta. Keskussairaalan lähiverkossa on käytössä noin kymmenisen eri virtuaalilania ja niitä joutuu kytkinten portteihin muuttelemaan lähes päivittäin. Lääkintälaitteet, työasemat, IP-kamerat ja muut verkon laitteet ovat jaoteltu karkeasti omiin virtuaalilaneihinsa, ja niiden fyysisten paikkojen vaihtelu ja muutokset aiheuttavat aina kytkinten päässä manuaalista työtä.

Jos verkosta täytyy löytää tietokone tai muu verkkolaite ja käytössä on esimerkiksi vain koneen IP tai DNS–nimi, ei tätä voida kätevästi suoraa paikantaa. Työasemista on olemassa lista, jossa näkyy käytössä olevien

työasemien sijoituspaikat. Nämä listat tosin jäävät auttamattomasti päivittämättä sairaalalla jatkuvasti tapahtuvien tilamuutosten ja muuttojen myötä. Jos joku on vienyt langattoman laitteen alkuperäissijoituspaikastaan muualle, vaikkapa kotiinsa tai toiselle osastolle ei tätä laitetta ole helppoa etsiä. LAN–verkossa olevat laitteet paikallistetaan tällä hetkellä manuaalisesti selvittämällä ensin reititystauluista laitteen MAC–osoite, jonka avulla kytkimen portti jossa laite on kiinni löytyy. Tämä on hidas, mutta nykyisellään myös ainut tapa paikantaa laite varmuudella.

3.3 Tietoturvariskit nykyisellä verkkoarkkitehtuurilla

3.3.1 LAN–verkon tietoturvariskit

-

3.3.2 WLAN–verkon tietoturvariskit

-

3.4 Raportoitavuus ja näkyvyys

Nykyisellään raportoitavuus rajoittuu lähinnä Neteye-ohjelmiston tuottamaan dataan verkosta. Qentinel NetEye valvoo ICT-palveluja, verkkoa sekä antaa yleisnäkymän ICT-palveluiden tuottamiseen liittyvien resurssien tilasta. Neteyella valvotaankin lähinnä tukiasemien ja kytkinten vastaamista ICMP pingiin, runkolinjojen pakettihävikkiä sekä palvelimissa lisäksi prosessorin ja muistin kuormitusta. Hälyytysrajojen ylittyessä tai pingin katketessa vastuuhenkilöille lähetetään sähköposti sekä sms-viesti, jossa hälyytys kuvaillaan.

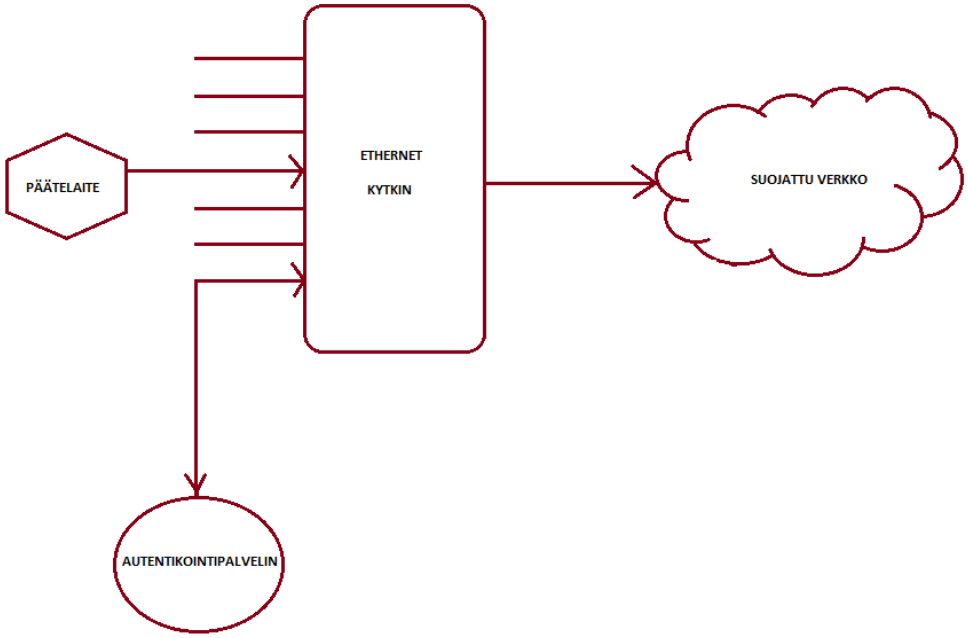
Loppukäyttäjän ongelmia on vaikea todentaa jos ei itse ole juuri silloin paikalla. Käyttäjän ilmoittamia verkko-ongelmia selvitettäessä päädytäänkin usein kaivelemaan Windowsin tapahtumalokia, jotta saadaan edes jonkinlainen käsitys tapahtuneesta. Reaaliaikaista seurantaa langattomien päätelaitteiden toiminnasta ei ole, joten WLAN-verkon pätkinnästä tulevat vikailmoitukset ovatkin lähes mahdottomia selvittää.

4 IEEE 802.1X STANDARDI

4.1 Yleistä standardista

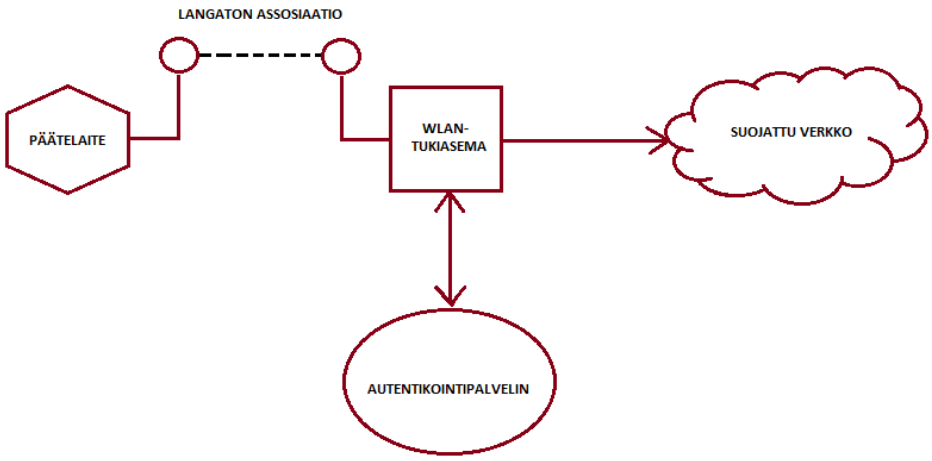
802.1x on IEEE-standardi porttikohtaiselle todentamiselle LAN- ja WLAN-verkoissa. Sen avulla voidaan autentikoida laitteita joille halutaan pääsy verkkoresursseihin sekä kokonaan estää luvattomien laitteiden pääsy verkkoon tai vaihtoehtoisesti ohjata ne esimerkiksi vierasverkkoon.

IEEE 802.3 -verkkoon liityttäessä jossa on käytössä 802.1X-todentaminen, päätelaite esittelee aluksi autentikointitietonsa autentikaattorille eli ethernet kytkimelle, joka varmistaa nämä tiedot todeksi autentikointipalvelimelta. Autentikointipalvelin käsittelee saadut tiedot ja tekee päätöksen siitä päästetäänkö laite verkon suojatulle alueelle vai ei. Tätä kutsutaan autorisoinniksi. (IEEE Std 802.1X-2010, 2)



Kuva 3. LAN-verkossa tapahtuva 802.1x todentaminen.

IEEE 802.11 verkkoon liityttäessä päätelaite suorittaa 802.1X autentikoinnin sen tukiaseman loogisessa portissa, johon se on kiinnittyneenä. Tästä eteenpäin autentikaatioprosessi etenee kuten lankaverkossakin.



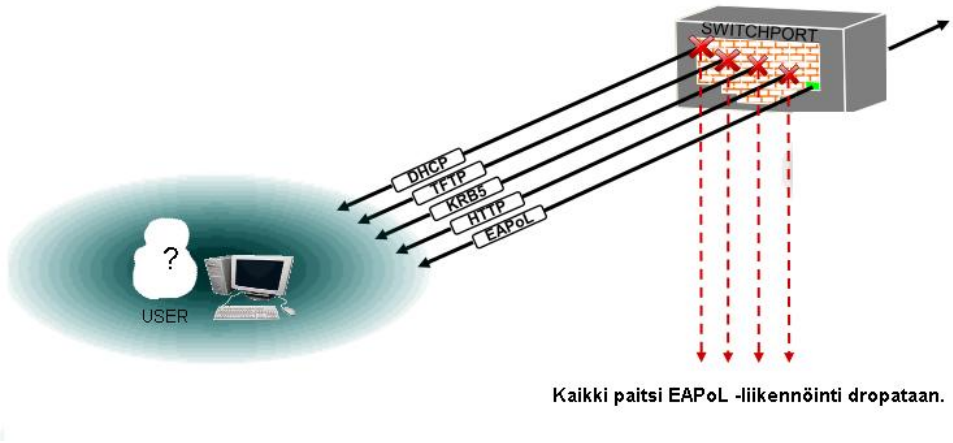
Kuva 4. WLAN-verkossa tapahtuva 802.1X todentaminen.

4.1.1 Supplikantti

Supplikantti on päätelaite jonka pitää autentikoitua ennen kuin se päästetään verkon suojatulle puolelle. Se voi esimerkiksi olla IP-puhelin, kannettava tietokone tai vaikkapa tabletti, joka tukee 802.1X:ää ja tiettyä EAP-Metodia. Windows XP:ssä on esimerkiksi oma natiivi 802.1X ohjelmisto sisäänrakennettuna sekä useita EAP-Metodeja kuten EAP-TLS ja EAP-MS-CHAP-V2. Supplikantti kommunikoi autentikointiserverin kanssa käyttäen EAP:aa tiedon kuljettamiseen ja EAP-Methodia itse autentikointiin. Kommunikointi itse autentikaattorin kanssa mahdollistetaan EAPoL:lla. (Geier 2008, 20, 39. IEEE Std 802.1X-2010, 9)

4.1.2 Autentikaattori

Autentikaattoriksi kutsutaan verkossa olevaa Layer 2-laitetta. Laite voi olla joko ethernet-kytkin tai langaton tukiasema. Autentikaattori toimii porttina supplikantin ja suojatun verkon välillä. Autentikaattorin portti pysyy kiinni niin kauan kunnes järjestelmä saa varmistettua supplikantin autentikointitiedot oikeellisiksi. Tätä ennen portista ei pääse läpi kuin EAPOL-liikenne kuten kuvasta 5 voimme nähdä. Jos autentikointi onnistuu, portti avataan ja supplikantti päästetään suojattuun verkkoon.



Kuva 5. Liikennöinti ennen onnistunutta autentikaatiota.. (Cisco 2011, BRKSEC-2005 - Deploying Wired 802.1x)

Autentikaattori toimii myös eräänlaisena tulkkina supplikantin ja autentikointipalvelimen välissä. Kun supplikantti ja autentikointipalvelin keskustelevat kaikki tämä liikenne kulkee autentikaattorin kautta. Autentikaattori prosessoi EAPoL-kehyksiä joiden sisällä EAP-Method-data sijaitsee. Tuloksena autentikaattorin kohdalla EAPoL-kehys puretaan ja EAP-Method -data kapseloidaan RADIUS-kehykseen datan kulkiessa supplikantilta palvelinta kohti. Prosessi tapahtuu päinvastoin palvelimelta supplikantille kommunikoidessa. (Geier 2008, 39. IEEE Std 802.1X-2010, 6)

4.1.3 Autentikointipalvelin

Porttikohtaiset autentikointistandardit ja spesifikaatiot eivät määrittele mitään tiettyä autentikointipalvelintyyppiä pakolliseksi, mutta silti lähes kaikki implementaatiot käyttävät Radiusta. Autentikointipalvelin on määritelty autentikaattorille. Usein käytössä on myös toissijaisia autentikointipalvelimia joita käytetään jos ensisijainen on syystä tai toisesta alhaalla. Joissain tapauksissa autentikointipalvelin on liitetty itse autentikaattoriin. Tätä tapaa voidaan käyttää esimerkiksi pelkästään langattomissa verkoissa autentikointiliikenteen rajoittamiseksi tai pienissä LAN-verkoissa taloudellisten kustannusten pienentämiseksi. (Geier 2008, 39. IEEE Std 802.1X-2010, 6)

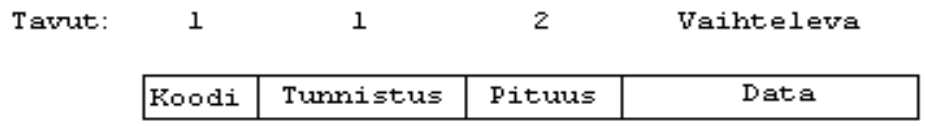
4.2 EAP

EAP eli Extensive Authentication Protocol on protokolla jota käytetään autentikointitiedon liikennöinnissä autentikointiprosessin eri osapuolten välillä. EAP ei yksinänsä ole itse autentikointiprotokolla tai autentikointimetodi, vaan standardi miten autentikointitiedot liikkuvat supplikantin, autentikaattorin ja autentikointipalvelimen välillä. EAP tukee erilaisia autentikointiprotokollia kuten EAP-TLS ja EAP-MS-CHAP-V2 joita käsitte-

lemme myöhemmin. (Geier 2008, 51. IEEE 802.1X/NAC Technology & Solution TOI, Mitsunori Sagae 2007, 29)

4.2.1 EAP-paketin koostumus

EAP-paketti koostuu koodi-, tunnistus-, pituus- ja dataosasta.



Kuva 6. EAP-paketti.

Koodiosa

Koodiosa tunnistaa minkä tyyppinen EAP-paketti on. Tämä osa on yhden tavun mittainen. Koodiosassa voidaan määritellä neljä erilaista tyyppiä EAP-paketille:

```
EAP-Request          0000 0001 (Hex ”01”)
EAP-Response         0000 0010 (Hex ”02”)
EAP-Success          0000 0011 (Hex ”03”)
EAP-Failure          0000 0100 (Hex ”04”)
```

Tunnistusosa

Tunnistusosa on myös yhden tavun mittainen. Tunnistusosalla oikeat EAP-Request ja EAP-Response-paketit sovitetaan yhteen.

Pituusosa

Pituusosa on kaksi tavua pitkä ja se sisältää tiedon koko EAP-paketin yhteenlasketusta pituudesta. Tämä koostuu siis koodi-, tunnistus-, pituus- ja dataosan summapituudesta. Jos esimerkiksi supplikantti vastaanottaa EAP-paketin, joka on 2335 tavua pitkä, mutta pituusosassa on tieto 2334 tavua on supplikantin pudotettava paketti ilman sen kummempia kysymyksiä.

Dataosa

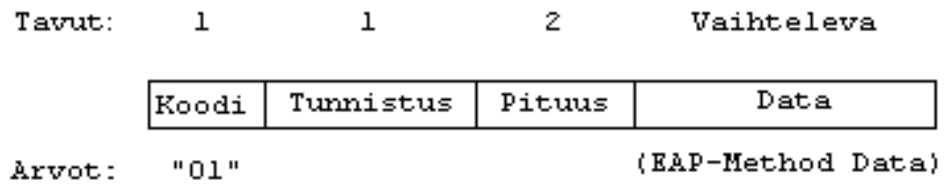
Dataosan sisältö riippuu EAP-paketin tyypistä. Esimerkiksi EAP-Request ja EAP-response-paketit omaavat dataosan. Aina dataosassa ei ole ollenkaan sisältöä.

(Geier 2008, 63, 64.)

4.2.2 EAP-pakettityypit

EAP-Request

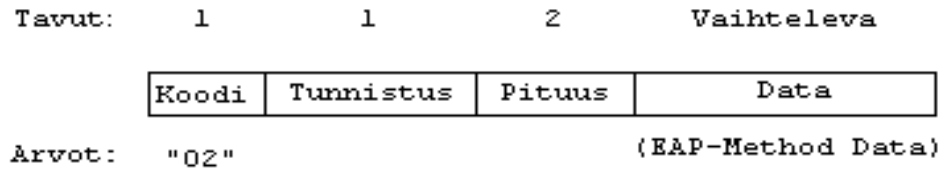
Autentikaattori kommunikoi supplikantin kanssa käyttäen EAP-Request -paketteja. EAP-Request-paketilla autentikaattori voi esimerkiksi pyytää supplikantilta identitettiä.



Kuva 7. EAP-Request-paketti. Paketti saa heksa-arvon ”01”.

EAP-Response

EAP-Response –paketteja käytetään niinikään supplikantin ja autentikaattorin kommunikointiin. EAP-Response-paketti lähetetään vastauksena EAP-Request-paketille.



Kuva 8. EAP-Response-paketti. Paketti saa heksa-arvon ”02”.

EAP-Response ja EAP-Request-tyypit

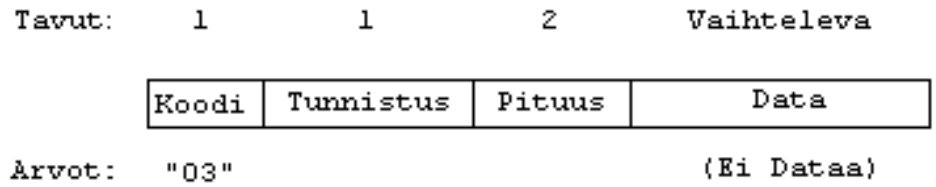
ARVO (binäärinen)	EAP TYYPPI
1 (0000 0001)	Identity
2 (0000 0010)	Notification
3 (0000 0011)	NAK
4 (0000 0100)	MD5-Challenge
5 (0000 0101)	One-Time Password
6 (0000 0110)	Generic Token Card
254 (1111 1110)	Expanded Types
255 (1111 1111)	Experimental use

EAP-Tyypit sijaitsevat EAP-Methods-paketin dataosassa.

Kuva 9. EAP-Method-paketti.

EAP-Success

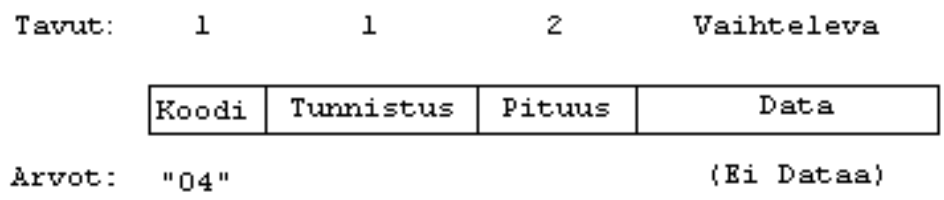
Jos autentikaattori saa palvelimelta päin tiedon onnistuneesta autentikoinnista lähettää se EAP-Success-paketin supplikantille ja tämä päästetään liikennöimään verkon suojatulle alueelle. Paketin dataosassa ei sisällä mitään vaan koodiosan heksa-arvo ”03” riittää onnistumisen ilmoittamiseen.



Kuva 10. EAP-Success-paketti. Paketti saa heksa-arvon ”03”.

EAP-Failure

Jos supplikantin autentikointiprosessin tuloksena autorisointia suojatun verkon puolelle ei myönnetä, lähetetään supplikantille EAP-Failure-paketti.

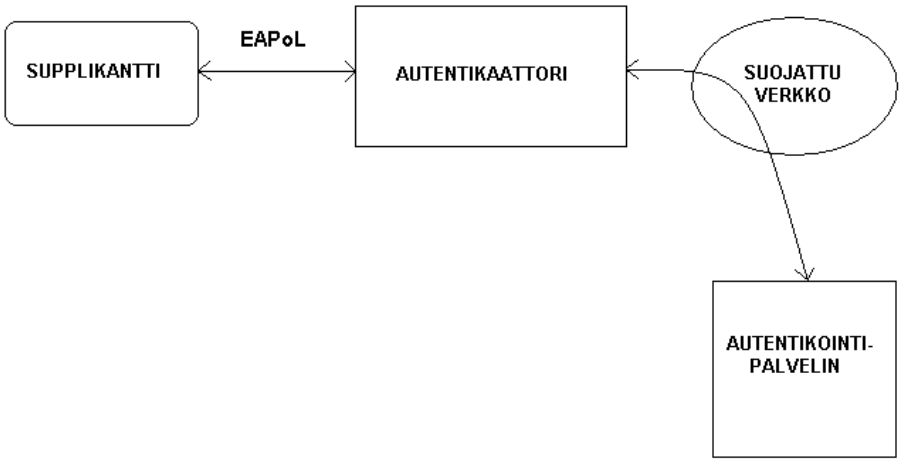


Kuva 11. EAP-Failure-paketti. Paketti saa heksa-arvon ”04”.

(Geier 2008, 64-67.)

4.3 EAPoL-protokolla

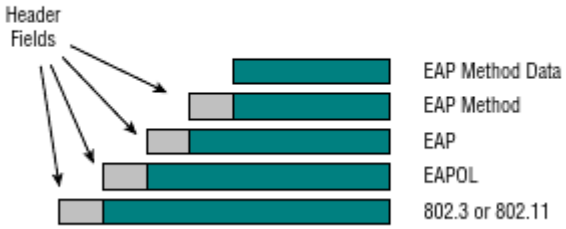
EAPoL eli Extensible Authentication Protocol over LAN on määritelty 802.1X-standardissa ja sen avulla EAP-paketteja siirrellään lähiverkoissa supplikantin ja autentikaattorin välillä kuvan 12 mukaisesti. EAP-paketit kuljetetaan EAPoL-paketin dataosassa. EAPoL toimii OSI layer 2:lla jotta estetään supplikantin pääsy verkkoon ennen autentikointia. (Geier 2008, 55, 56.)



Kuva 12. EAPoL kommunikointi tapahtuu supplikantin ja autentikaattorin välillä.

4.3.1 EAPoL kapselointi

Porttikohtaisessa autentikoinnissa tapahtuvan liikennöinnin tärkein tehtävä on kuljettaa EAP-Method dataa, jonka sisällä itse autentikaatiotieto sijaitsee. Käytössä oleva EAP-Metodi määrää tuon autentikointitiedon (EAP-Data) sisällön. EAP-Request ja -Response -paketit kuljettavat EAP-Method -headereita ja dataa. EAP-Request ja –Response-paketteja taas kuljettaa EAPoL. Lopuksi 802.3 tai 802.11 datakehykset siirtävät EAPoL paketit. Kuvassa 13 on esitetty tämä kapselointi kokonaisuudessaan.



Kuva 13. Supplikantin ja autentikaattorin kesken suoritettava kapselointi. (Geier 2008, 56)

4.3.2 EAPoL-paketin koostumus

EAPoL lisää EAP-paketteihin kolme lisäosaa. Nämä lisäosat mahdollistavat EAP-pakettien siirron lähiverkoissa.

Tavut:	1	1	2	Vaihteleva
	Versio	Tyyppi	Pituus	Runko-osa

Kuva 14. EAPoL-paketti.

Versio-osa

EAPoL-paketin versio-osassa määritellään paketin lähettäjän käyttämä EAPoL-protokollaversio. 802.1X:ää käytettäessä versio-osa sisältää aina arvon ”0000 0010” eli heksa-arvona ”2” ja on yhden tavun mittainen.

Tyyppiosa

Tyyppiosakin on pituudeltaan yhden tavun mittainen. Se määrittelee lähetetyn paketin tyypin. Tällä hetkellä EAPoL tyyppejä ei ole kuin alla mainitut viisi, mutta tulevaisuudessa tämä voi muuttua.

TYYPPI	TYYPPIOSAN ARVO
EAP-Packet	0000 0000 (Hex ”00”)
EAPoL-Start	0000 0001 (Hex ”01”)
EAPoL-Logoff	0000 0010 (Hex ”02”)
EAPoL-Key	0000 0011 (Hex ”03”)
EAPoL-Encapsulated-ASF-Alert	0000 0100 (Hex ”04”)

Pituusosa

Pituusosa EAPoL-paketissa on kahden tavun mittainen. Se ei määrittele koko paketin pituutta kuten EAP-paketissa, vaan ainoastaan runko-osan pituuden. Arvo joka pituusosa sisältää kertoo kuinka monta tavua runko-osa on. Esimerkiksi EAPoL pituusosan arvo ”0000 0000 0011 0111” kertoo runko-osan kooksi 55 tavua. Arvo on nolla EAPoL-Start ja EAPoL-Logoff-paketeissa. Itse EAPoL-paketin maksimipituus riippuu kuljetusprotokollien kuten IEEE 802.3 ja 802.11 rajoituksista.

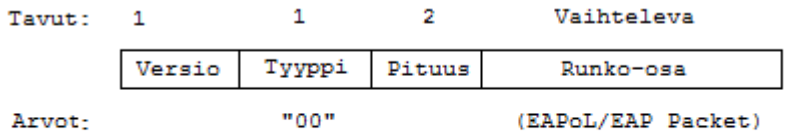
Runko-osa

Runko-osassa sijaitsee EAPoL-paketin hyötykuorma. Jos paketin tyyppi on ”EAP-Packet”, on hyötykuormana tasan yksi EAP-paketti. Jos paketin tyyppi on esimerkiksi EAPoL-Key, sisältää hyötykuorma yhden avainsanan (Key Descriptor). (Geier 2008, 57-59.)

4.3.3 EAPoL-pakettityypit

EAP-Packet

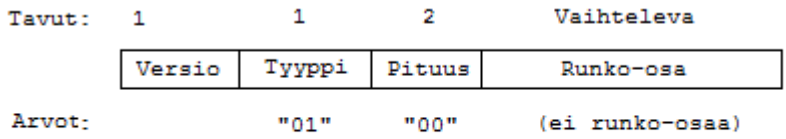
EAPoL-pakettityyppi EAP-Packet sisältää yhden EAP-paketin. EAP-Packetista käytetään myös termejä ”Type-0-EAPoL packet” tai ”EAPoL-data packet”. Supplikantti tai autentikaattori poistaa EAP-Packetista EAPoL-headerin ja käsittelee EAP-paketin. Näinollen ”Type-0-EAPoL” paketit vain siirtelevät, lähinnä EAP-Method dataa sisältäviä EAP-paketteja, edestakaisin.



Kuva 15. EAPoL EAP-Packet.

EAPoL-Start

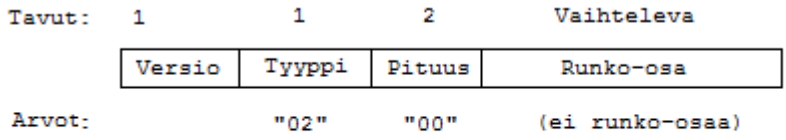
Kun tietoliikennelinkki nousee ylös, alkaa autentikointiprosessi. Supplikantti käynnistää autentikointiprosessin lähettämällä EAPoL-Start-paketin autentikaattorille joka jatkaa tästä supplikantin autentikointia.



Kuva 16. EAPoL-Start-paketti. Hex-arvo “01”

EAPoL-Logoff

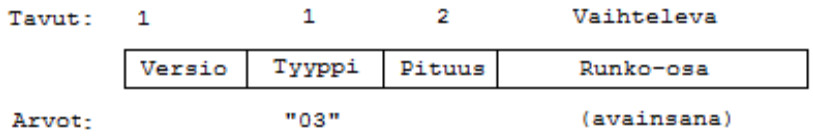
Kun supplikantti päättää katkaista yhteyden suojattuun verkkoon, lähettää se kuvassa 17 esitetyn paketin autentikaattorille. Autentikaattori muuttaa paketin saatuaan kyseisen portin autorisoimattomaan tilaan ja sitä ei aukaista ennen kuin uusi autentikaatio on suoritettu onnistuneesti loppuun.



Kuva 17. EAPoL-Logoff-paketti. Paketti tunnistetaan tyyppiosan hex-arvosta ”02”

EAPoL-Key

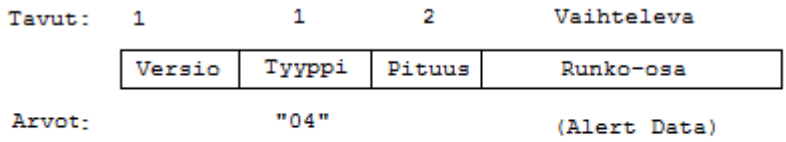
EAPoL-Key-paketin voi lähettää joko autentikaattori tai supplikantti. Tämä paketti ei ole pakollinen, vaan sen käyttö määritellään erikseen eri 802.1X implementaatioissa. Jos kyseinen implementaatio vaatii avainten käytön, sisältää EAPoL-Key-paketin runko-osa sen.



Kuva 18. EAPoL-Key-paketti. “Key Descriptor” eli avainsanatieto sijaitsee runko-osassa.

EAPoL-Encapsulated-ASF-Alert

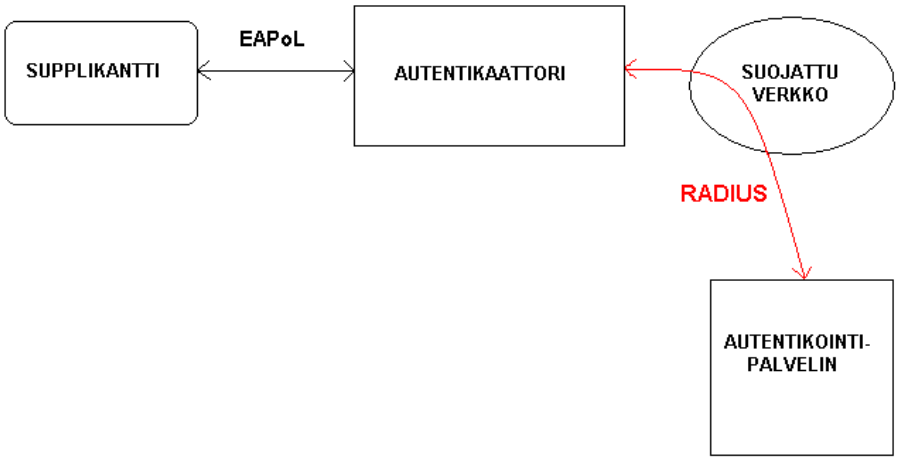
Tätä pakettia käytetään jos ja kun supplikantin täytyy lähettää tietoa verkon suojatulle puolelle ennen autentikoinnin päätöstä. Tällainen voi olla esimerkiksi status-viesti palvelimelle. Tällaiset viestit ovat yleensä valmistajakohtaisia. (Geier 2008, 59-62)



Kuva 19. EAPoL-Encapsulated-ASF-Alert –paketti. Tämä tunnistetaan tyyppiosan heksa-arvosta ”04”.

4.4 RADIUS-protokolla

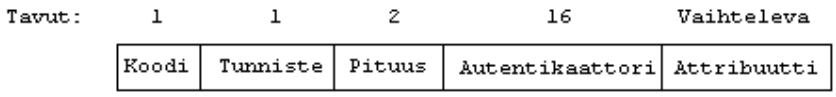
RADIUS on nykypäivänä yleisin autentikointipalvelinten käyttämä protokolla. RADIUSTA käytetään autentikoinnin suorittavan palvelimen ja autentikaattorin välisessä kommunikoinnissa kuten kuvassa 20 esitetään. RADIUS kuljettaa EAP-Method-dataa kryptatussa muodossa. Seuraavaksi käsittelemme radiuksen yleisimpiä ominaisuuksia. (Geier 2008, 71)



Kuva 20. RADIUSTA käytetään autentikointipalvelimen ja autentikaattorin välillä.

4.4.1 RADIUS-paketin koostumus

Kaikki RADIUS-paketit ovat peruskoostumukseltaan samanlaisia. Ne koostuvat koodi-, tunnistus-, pituus-, autentikaattori- ja attribuuttiosista.



Kuva 21. RADIUS-paketin koostumus.

Koodiosa

Koodiosa on yhden tavun mittainen ja siitä selviää radius –paketin tyyppi.

KOODI	PAKETIN TYYPPI
1	RADIUS Access-Request
2	RADIUS Access-Accept
3	RADIUS Access-Reject
4	RADIUS Accounting-Request
5	RADIUS Accounting-Response
11	RADIUS Access-Challenge
12	Status-Server (kokeiluasteella)
13	Status-Client (kokeiluasteella)
255	Reserved

Tunnisteosa

Tunnisteosa on myös pituudeltaan yhden tavun ja aivan kuten EAP-protokollassa tällä saatetaan yhteen oikeat Access-Challenge- ja Access-Request-paketit.

Pituusosa

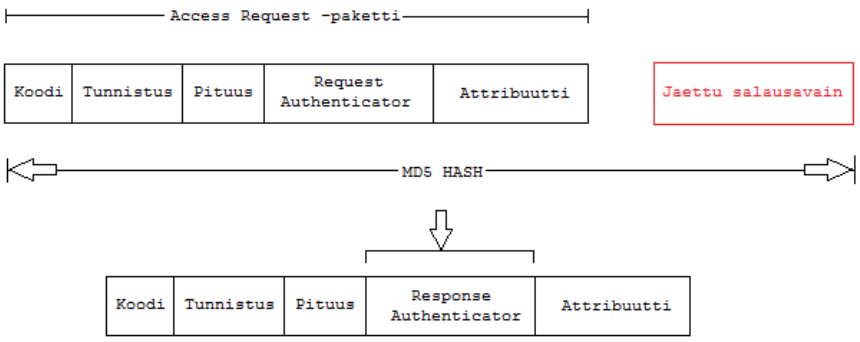
RADIUS-paketin pituus on kaksi tavua pitkä ja siinä määritellään, kuten EAP-paketissakin, kyseisen paketin kokonaispituus. Suurin mahdollinen pituus on 4096 tavua. Jos pituusosassa määritelty pituus ei vastaa paketin todellista kokoa tulee se yksiselitteisesti hylätä.

Autentikaattoriosa

Tämä osa koostuu 16 tavusta ja on hieman erilainen riippuen onko se tyypiltään ”Request Authenticator” vai ”Response Authenticator”

Access-Request-paketeissa autentikaattoriosa koostuu ”Request Authenticator”-arvosta. Tämä arvo on ennalta määräämätön satunnaisluku. Autentikaattoripalvelimen ja autentikaattorin jaettu salausavain yhdistetään ”Request Authenticator”-arvon kanssa ja viedään MD5 hashin läpi josta saadaan 16 tavua pitkä luku. Tämä yhdistetään loogisella operaattorilla XOR (exclusive or) käyttäjän salasanan kanssa. Access-Request-paketti tallettaa tämän luvun ”user-password”-arvoksi.

“Response Autheticator” sijaitsee Access-Accept-, Access-Reject-, ja Access-Challenge-pakettien autentikaattoriosassa. Response Authenticator on salausavaimen kanssa MD5 hashin läpi viety vastaava radius ”Access Request” –paketti. Kuva 22 selventää tätä monimutkaista asiaa paljon.



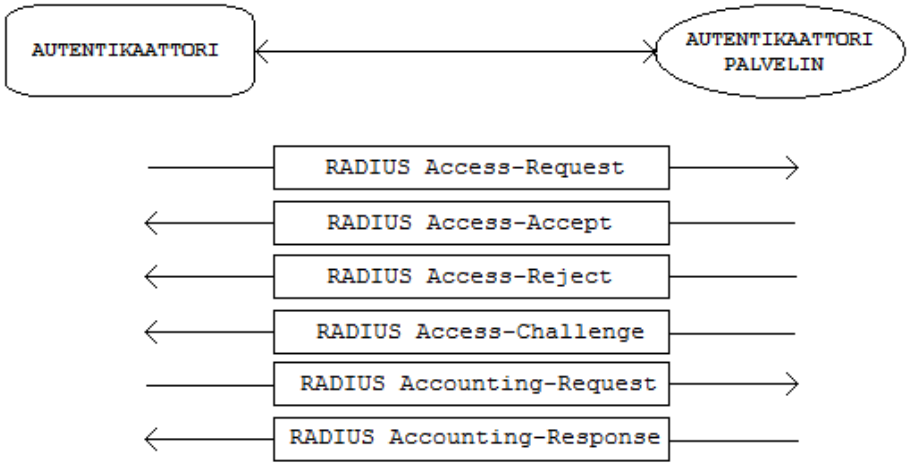
Kuva 22. Eri autentikaattoriosat

Attribuuttiosa

RADIUS-paketin attribuuttiosassa on dataa joita käytetään autentikaattorin ja autentikointipalvelimen kommunikoinnissa. Sen pituus vaihtelee. Attribuutteja on 44 erilaista (40-59 varattu accountingia varten) käyttäjätunnuksista ja salasanoista porttirajoituksiin. (Geier 2008, 72-76)

4.4.2 RADIUS-paketin tyypit

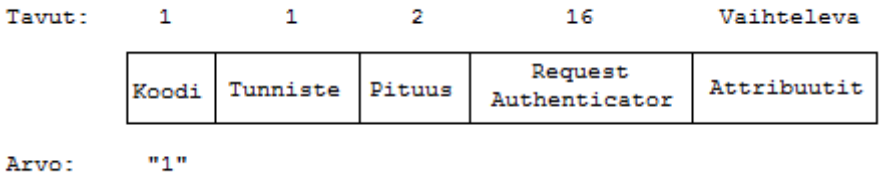
RADIUS-paketteja on käytössä kuutta tyyppiä. Kuvassa 23 on esitetty kaikki kuusi, sekä niiden kommunikointisuunnat.



Kuva 23. RADIUS-pakettityypit suuntineen.

RADIUS Access-Request

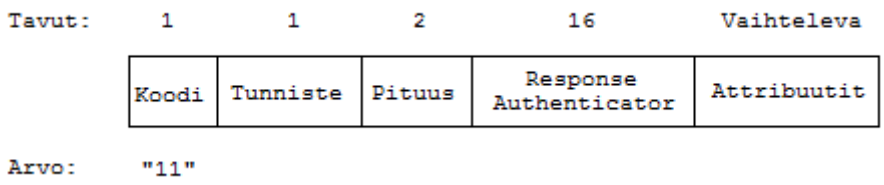
Access-Request lähetetään autentikaattorilta autentikointipalvelimelle. Se sisältää käytössä olevaan EAP-methodiin perustuvaa dataa. Aina supplikanttia autentikoitaessa käytetään ensiksi Access-Requestia ja se voi sisältää esimerkiksi käyttäjänimen.



Kuva 24. RADIUS Access-Request –paketti.

RADIUS Access-Challenge

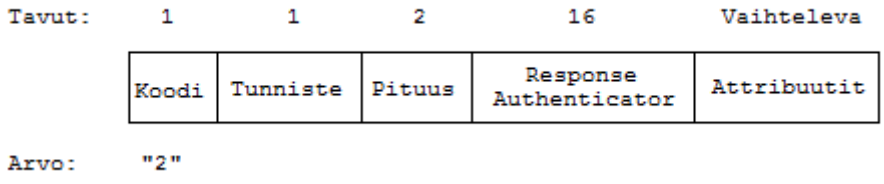
Tämä paketti lähetetään autentikointipalvelimelta autentikaattorille vastauksena Access-Request-pakettiin ja näiden tunnisteosan tulee vastata toisiaan. Attribuuttiosa voi sisältää arvoja ”State”, ”Reply-Message”, ”Vendor-Specific”, ”Idle-Timeout”, “Session-Timeout” ja “Proxy-State”.



Kuva 25. RADIUS Access-Challenge-paketti.

RADIUS Access-Accept

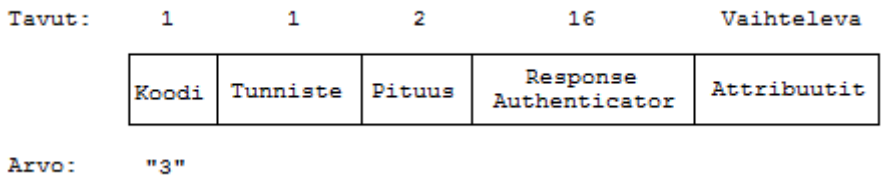
Tämä paketti lähetetään myös palvelimelta autentikaattorille vastauksena Access-Requestiin. Se voi sisältää esimerkiksi konfiguraatiotietoa supplikantille. Samoin kuin Access-Challenge-paketissa, tunnisteosien on täsmättävä Accept-Request-paketin kanssa. Attribuuttiosa sisältää samankaltaisia tietoja, kuin Accept-Challenge-pakettikin.



Kuva 26. RADIUS Accept-Access –paketti.

RADIUS Access-Reject

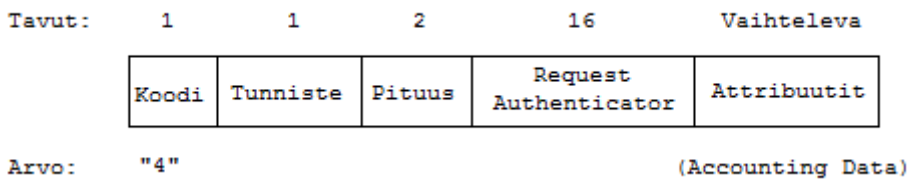
Access-Reject-paketti lähetetään autentikointipalvelimelta autentikaattorille silloin, kun Access-Request –paketin attribuutit eivät ole hyväksyttäviä. Tunnisteosan on jälleen vastattava Access-Request paketin tunnisteosaa. Attributtiosassa voi olla esimerkiksi selkokielinen teksti, jonka autentikaattori voin esittää käyttäjälle merkkinä epäonnistuneesta autentikaatiosta.



Kuva 27. RADIUS Access-Reject-paketti.

RADIUS Accounting-Request

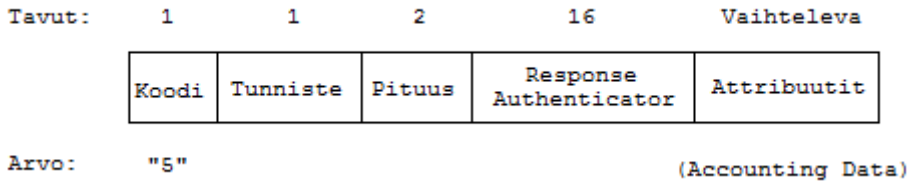
Accounting-Request-paketti lähetetään autentikaattorilta palvelimelle, jos tarvitaan accounting-tietoa.



Kuva 28. RADIUS Accounting-Request-paketti.

RADIUS Accounting-Response

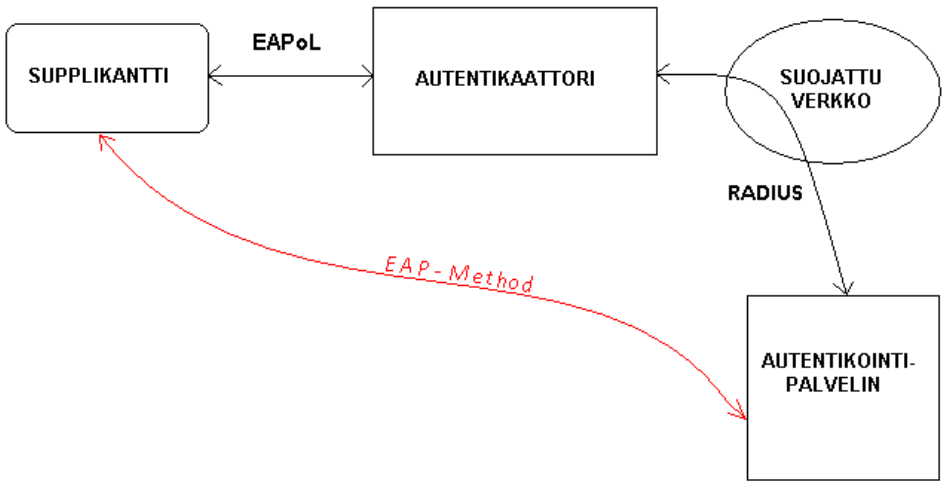
Autentikointipalvelin lähettää tämän paketin vastauksena autentikaattorin Accounting-Request-kyselyyn. Tunnistekenttien on vastattava toisiaan tai paketti pudotetaan. (Geier 2008, 76-79)



Kuva 29. RADIUS Accounting-Response-paketti.

4.5 EAP-Methods-protokolla

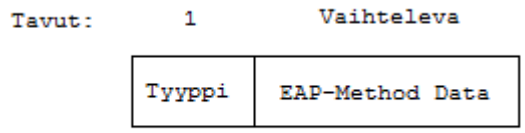
EAP-Methods-protokollaa käytetään kuvan 30 mukaan päätepisteiden eli supplikantin ja autentikointipalvelimen välisessä kommunikoinnissa. EAP-Methodsista käytetään myös nimitystä ”EAP type” tai ”EAP tyyppi”. EAP-Methods sisältää itse autentikointiprosessin tiedot, EAPoL:a ja Radiusta käytetään tämän tiedon eli EAP-Methods datan kuljeukseen. (Geier 2008, 93)



Kuva 30. EAP-Method kulkee aina supplikantilta autentikointipalvelimelle asti.

4.5.1 EAP-Method -paketin koostumus

Kaikilla EAP-Method -paketeilla on samanlainen peruskoostumus, johon kuuluvat tyypposa ja EAP-Method dataosa. Tämä paketti kuljetetaan EAP-paketin dataosassa.



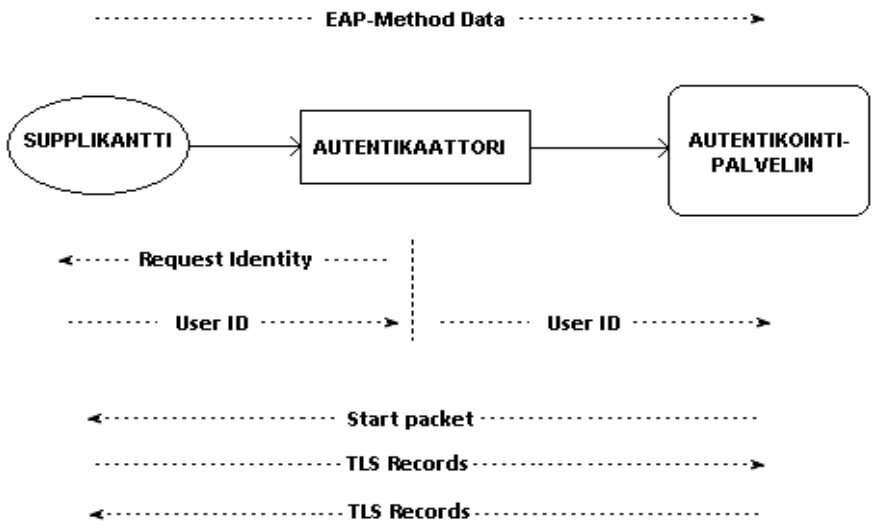
Kuva 31. EAP-Method-paketin koostumus.

EAP-Method typpiosa

Tyyppiosa on yhden tavun kokoinen. Sen sisältämä binääriluku kertoo, mikä EAP-Method on käytössä. Erilaisia EAP-Methodeja on lähes 50 erilaista, joten käymme tarkemmin läpi vain sairaalalla testatut tyypit EAP-TLS ja PEAP.

EAP-TLS (Extensible Authentication Protocol with Transport Layer Security) on EAP-Method tyyppi numero 13. TLS:llä molemmat sekä supplikantti, että autentikointi palvelin todistavat identiteettinsä. EAP-TLS käyttää hyväkseen sertifikaatteja joten tämä on mainio vaihtoehto yrityksille, joilla on jo valmiiksi CA-palvelut toiminnassa. Kommunikaatio supplikantin ja palvelimen välillä toteutetaan kryptatulla TLS-tunnelilla. Sertifikaatit asennetaan sekä supplikantille, että palvelimelle. Sertifikaattien asentamisesta jokaiselle työasemalle aiheutuukin EAP-TLS:n käyttööotossa suurin työ.

PEAP (Protected Extensible Authentication Protocol) on Microsoftin, Ciscon ja RSA Securityn kehittämä protokolla, ja sitä tarjotaan käyttäjille ilmaiseksi. PEAP on EAP-Method tyyppi numero 25. PEAP ei tarvitse sertifikaatteja supplikantin päähän, vaan pelkästään autentikointipalvelimelle. Autentikointidata tunneloidaan palvelimen ja supplikantin välillä.



Kuva 32. EAP-TLS-autentikointi.

EAP-Method dataosa

Dataosa voi sisältää erilaista tietoa riippuen EAP-Method-tyypistä ja käytetyistä protokollista. Siellä voi olla esimerkiksi käytössä oleva digitaalinen sertifikaatti matkalla supplikantilta autentikointipalvelimelle. (Geier 2008, 95-6)

5 IDENTITEETTITIETOINEN VERKKOARKKITEHTUURI

5.1 Mitä on identiteettitietoinen verkkoarkkitehtuuri

Identiteettitietoinen verkkoarkkitehtuuri on sitä, että verkko suunnitellaan ja rakennetaan sen pohjalta, että käyttäjän identiteetti on tiedossa ja varmistettu, ennen kuin hänelle annetaan minkäänlaisia oikeuksia käyttää verkkoa. Identiteetti määritelmänä vaihtelee hieman riippuen siitä, mikä on kunkin yrityksen haluttu tietoturvataso. Sairaaloissa tietoturva ja varsinkin potilastietoturva on hyvin tärkeää, joten jokainen sairaalan turvattua verkkoa käyttävä halutaan tunnistaa mahdollisimman tarkasti. Enää ei tyydytä tunnistamaan ”käyttäjää” pelkän konenimen, IP- tai MAC-osoitteen avulla, vaan identiteetti halutaan varmistaa itse käyttäjää myöden. Identiteetti tarkoittaakin yhdessä kaikkea sitä, että ymmärretään ennen oikeuksien antamista kuka tai mikä pyrkii verkkoon, missä se sijaitsee sekä koska tai miten se päästetään verkon suojatulle alueelle.

Identiteettitietoiseen verkkoarkkitehtuuriin liittyykin kiinteästi kolme käsitettä: autentikointi, autorisointi ja tilastointi. Autentikoinnilla tarkoitetaan käyttäjän ja hänen käyttöoikeuksiensa tunnistamista. Autorisoinnilla tai valtuutuksella käyttäjä ohjataan autentikointiin perustuen käyttämään oikeita verkon palveluita ja resursseja. Käyttäjä voidaan valtuuttaa käyttämään esimerkiksi vain tiettyä virtuaalilania. Tilastoinnilla eli accountingil-

la pidetään kirjaa verkossa toimivien käyttäjien tiedoista ja esimerkiksi olinpaikoista ja yhteysajoista. Tilastointitietoja voidaan käyttää vikatilanteiden tai tietoturva-aukkojen kartoittamiseen.

5.2 Hyödyt verrattuna nykyiseen verkkoarkkitehtuuriin

Nykyiseen verkkoarkkitehtuuriin verrattuna identiteettitietoinen verkkoarkkitehtuuri 802.1X:llä ja Ciscon Trustsec –kokoonpanolla varustettuna toisi lisää tietoturvaa, helppokäyttöisyyttä ja raportointimahdollisuuksia. Jokapäiväinen kytkinporttien peruskonfigurointi vähenisi lähes olemattomiin dynaamisesti virtuaalilaneja vaihtavien ominaisuuksien myötä. Verkkopisteitä voisi jäädä aktiivisiksi, eivätkä ne silti muodostaisi huomattavaa tietoturvariskiä. Jos ulkopuolinen liittäisi laitteensa tuohon pisteeseen, ohjattaisiin hänet 802.1x autentikointiin perustuen joko vierailijaverkkoon tai pysäytettäisiin portin liikenne tyystin.

Langattoman verkon puolella tietoturva niin ikään kasvaisi. Myös avoimesta vierailijaverkosta päästäisiin eroon ja näin voitaisiin tarjota entistä parempaa suorituskykyä myös tätä verkkoa käyttäville. WLAN -ongelmien selvitys helpottuisi Prime verkon hallintajärjestelmällä. Langattomassa verkossa olevien laitteiden käyttäytymisestä voitaisiin nähdä historiatietoa, eikä paikanpäällä tarvisi olla aina vian sattuessa. Vikaa voitaisiin analysoida jälkikäteen Primen tuottamien raporttien avulla.

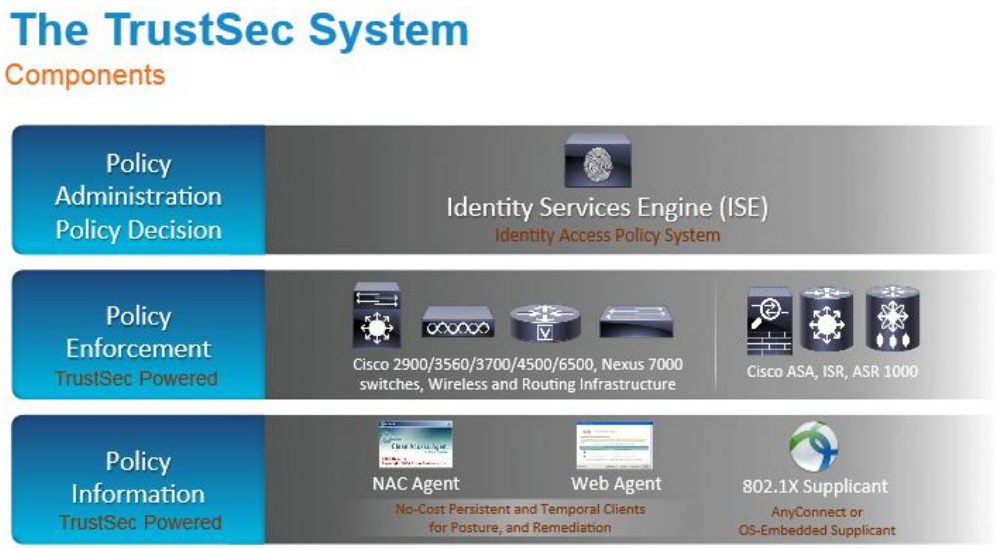
5.3 Haasteet uudella identiteettitietoisella verkkoarkkitehtuurilla

Suurimmiksi haasteiksi muodostuisivat laitteet jotka eivät tue 802.1.X standardia. Verkkotulostimet, lääkintälaitteet ja –järjestelmät. Miten saada tämä suuri joukko laitteita toimimaan uudenlaisessa järjestelmässä? Myöskään nykyinen verkkoinfrastruktuuri ei kaikilta osin tue 802.1X:n implementointia joten taloudellisiakin haasteita on odotettavissa.

5.4 Ratkaisuksi Cisco TrustSec

Cisco TrustSec on osa Ciscon SecureX arkkitehtuuria. Se on identiteettitietoinen pääsynhallintaratkaisu, joka pienentää tietoturvariskejä tarjoamalla täyden näkyvyyden siitä kuka, mikä ja milloin koittaa liittyä tietoverkon turvatulle alueelle sekä mahdollisuuden kontrolloida sitä, mitä tälle alueelle päästetyt voivat tehdä. IEEE 802.1X:n ja dynaamisen VLAN –kontrolloinnin lisäksi TrustSec tarjoaa ladattavia pääsylistoja (dACL:t), Security Group Accessin (SGA), koneprofilointia, tarkastus- ja raportointimahdollisuuden verkkoon liittyvän päätelaitteen tietoturvan nykytilasta sekä laajat vierasverkon hallintamahdollisuudet. Kanta-Hämeen Keskussairaalalle asennettava TrustSec-järjestelmä koostuu Ciscon Identity Services Enginestä (ISE), Wireless LAN Controllerista (WLC), Adaptive Security Appliance (ASA) Secure Access Control Systemistä (ACS), Prime Network Control Systemistä sekä Anyconnect-clientista. Käytössä jo valmiiksi oleva ja pääasiassa Ciscon Catalyst 3000-sarjan kytkimistä koostu-

va verkkoinfrastruktuuri sekä WLC, ACS ja ASA helpottavat ja nopeuttavat TrustSecin käyttöönottoa suuresti. (https://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_2.0/trustsec_2.0_dig.pdf)



Kuva 33. Ciscon TrustSec kokoonpano (www.cisco.com).

5.4.1 Cisco Identity Services Engine (ISE)

ISE on pääsynhallinta-alusta, joka käyttää pääsynhallintaan käyttäjän luomia erilaisia politiikoita. ISE:n arkkitehtuuri mahdollistaa yritysten kerätä reaaliaikaista informaatiota verkoista, niiden käyttäjistä ja laitteista. ISE voidaan sitoa erilaisiin verkkoelementteihin kuten kytkimiin, palomuureihin, WLAN-kontrollereihin ja VPN-keskittimiin joiden avulla loppukäyttäjien ja heidän käyttämiensä laitteiden identiteetti pyritään varmistamaan mahdollisimman tarkasti ja ohjaamaan heidät käyttämään haluttuja verkkoresursseja. ISE on koko tämän pääsynhallintajärjestelmän aivot, jotka ohjaavat muita verkkoresursseja siihen määriteltyjen politiikkojen mukaisesti.

ISE:n tarjoama identiteettipohjainen tunnistautuminen tarjoaa seuraavia ominaisuuksia:

- ISE ottaa selville pyrkiikö käyttäjä verkkoon autorisoidulla ja politiikkojen sallimalla laitteella.
- ISE pystyy luomaan historiatiedon käyttäjän identiteetistä, sijainnista sekä pääsynhallinnallisista päätöksistä raportointia ja järjestelmän toimivuuden tarkkailua varten.
- ISE myöntää palveluita perustuen käyttäjän rooliin, ryhmään ja käytössä olevaan politiikkaan (työtehtävä, käytetyn laitteen tyyppi, käyttöjärjestelmän suojaustaso jne.)
- ISE pystyy myöntämään autentikoiduille käyttäjille pääsyn tiettyihin verkkosegmentteihin tai tiettyihin ohjelmiin ja palveluihin tai molempiin, perustuen autentikoinnin tulokseen.

Perusperiaatteeltaan Cisco ISE tukee 802.1X:ää, MAC Authentication Bypassia (MAB) ja selainpohjaista autentikointia käyttäjän tunnistamiseen ja pääsynhallintaan sekä langattomissa että langallisissa lähiverkoissa. Autentikointipyynnön saatuaan ISE määrittää sallitut protokollat joita käytetään pyyntöä käsiteltäessä eteenpäin. Tämän jälkeen käyttäjää sekä tämän käyttämää laitetta (tai molempia) verrataan ISE:en määriteltyihin identiteettivarastoihin, kuten yrityksen active directoryyn, kunnes saadaan lopullinen autorisointi aikaiseksi.

Kun kysessä olevan istunnon autentikointi onnistuu siirtyy ISE määrittämään tälle autorisointi politiikkaa. Politiikka voidaan määrittää myös annettavaksi sellaisissa tapauksissa, joissa autentikointi epäonnistuu. Tällöin käyttöön voidaan ottaa esimerkiksi politiikka, joka ohjaa käyttäjän selainsivulle rekisteröitymään vierasverkkoon, eikä anna resursseja suojatun verkon puolelta. Onnistuneen autentikoinnin jälkeen käyttäjä autorisoidaan politiikaan perustuen verkon suojattuihin alueisiin. ISE:n yksi suurista vahvuuksista on niin kutsuttu monitorointi moodi. Tällä pystytään suorittamaan ja monitoroimaan 802.1X autentikointia ja autorisointia ilman, että käyttäjien käyttökokemus häiriintyy millään tavalla. Verkon ylläpitäjät voivat täten konfiguroida verkon laitteet toimintavalmiiksi ennen 802.1X:n varsinaista käyttöönottoa.
(http://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_overview.html)

5.4.2 Cisco Prime

Cisco Prime Infrastructure on hallintaratkaisu, jonka tarkoituksena on langallisen ja langattoman verkon käyttöönoton nopeuttaminen, pääsynhallinnan helpottaminen ja loppukäyttäjän käyttökokemuksen parantaminen.

Prime yhdistää loppukäyttäjän ja päätelaitteen identiteettitiedon sovellustason näkyvyyteen ja koko verkkoinfrastruktuurin hallintaan. Tämä lähestymistapa auttaa verkon ylläpitäjiä tehostamaan toimintaansa yksinkertaistamalla operointi- ja viestintämenetelmiään.

Primen toimintoja:

- Yhdistetty langallisen ja langattoman verkon aktiivilaitteiden hallinta ja valvonta reitittimiä myöden.
- Kattava verkkolaitteiden elinkaarenhallinta, mukaan lukien näkyvyyden loppukäyttäjätasolle asti, inventaarion- ja konfiguraatioversioitten hallinnan , autoprovisioinnin, radiorajapinnan kaistankäytön suunnittelun ja valvonnan, sekä verkkolaitteiden asetusten vertaamisem yleisesti alalla toimiviksi ja turvallisiksi todettuihin hyviin käytäntöihin.
- Sovellustason palvelulaadun seuranta, jonka avulla mahdolliset suorituskykyongelmat havaitaan ja korjataan nopeammin. Tähän hyödynnetään teknologioita kuten Network Based Application Recognition (NBAR2), NetFlow ja Medianet Performance Agent.

– 360 asteen näkymät, joissa yhdistetään kaikki tiettyä verkkolaitetta, päätelaitetta, tai käyttäjää koskevat tiedot ja työkalut yhteen selkeään yhteenvetoon.
– Uusien Cisco-teknologioitten käyttöönoton helpottaminen ja tehokas seuranta. Esimerkkeinä Cisco Adaptive wireless Intrusion Prevention System (wIPS), Cisco CleanAir, VPN, Zone-based Firewall, ScanSafe, ja Cisco Application Visibility and Control (AVC).

Cisco Prime on suunniteltu toimimaan myös erittäin suuria verkkokonaisuuksia silmällä pitäen. Se on mahdollista laajentaa jopa tuhansia verkkoelementtejä käsittäväksi hallintaratkaisuksi. Mahdollisuus integroituihin vikatiketti- ja raportointijärjestelmiin onnistuu REST-pohjaisen API-integrointirajapinnan kautta.

Primeen voidaan lisätä myös Mobility Services Engine, joka tarjoaa lisätoimintoja langattomien verkkojen puolelle:

– Paikkatietoisuuden lisääminen. Tarkoittaa päätelaitteiden, langattomien tietoturvauhkien, häiriölähteiden ja RFID-tekniikalla varustettujen elementtien paikannus, seuranta ja valvonta. Tätä tietoa voidaan hyödyntää myös muissa, esimerkiksi potilasturvallisuutta lisäävissä paikannuspalveluissa API-rajapinnan kautta.
– CleanAir-spektrianalysaattoritiedon tallennus ja analysointi. Radiorajapinnan häiriöiden ja niiden vaikutusalueen piirtäminen pohjakuviin. Vaatii CleanAir-toiminnalla varustetut tukiasemat.
– Järjestelmätason langattoman verkon tunkeutumisenestojärjestelmä Adaptive Wireless Intrusion Prevention System (wIPS).

(http://www.cisco.com/en/US/docs/net_mgmt/prime/network/3.10/user/guide/CiscoPrimeNetwork-UserGuide.html)

5.4.3 Cisco Anyconnect

Cisco Anyconnect on Cisco Systemssin kehittämä supplikantti, jolla voidaan hallita langatonta ja langallista verkkoa sekä VPN-yhteyksiä. Yksi ohjelmisto, jolla voi hoitaa kaikki tietokoneen yhteydet yksinkertaistaa toimintaa huomattavasti. Nykyisellään sairaalalla on käytössä omat supplikantit molemmille LAN ja WLAN yhteyksille sekä VPN:lle useampia.

Anyconnect-clienttiin luodaan xml-muotoiset profiilitiedostot ”Anyconnect Profile Editor”-nimisellä ohjelmalla. Nuo profiilit voidaan näppärästi tiputtaa GPO:na työasemaryhmille. Itse Anyconnectin voi jaella MSI-pakettina, jolloin se asentuu vaivatta halutuille työasemille. Opinnäytetyöhön ei sisälly VPN-clientin testausta. Todettakoon kuitenkin, että se on täysin yhteensopiva ASA5500-palomuurilaitteiston kanssa, ja todettu yksinkertaiseksi ja toimivaksi. Voidaan siis helposti ottaa käyttöön koska tahansa. Anyconnectin käytöstä tullaan testaamaan Windows 7 ja Windows XP-ympäristöt LAN- ja WLAN-yhteyksillä ja autentikointimuodoista samat kuin natiiveilla supplikanteillakin eli EAP-PEAP ja EAP-TLS.

(http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/anyconnectadmin30.html)

6 TOTEUTUS

6.1 Yleistä

Identiteettitietoisen verkkoarkkitehtuurin rakentaminen päätettiin aloittaa Cisco Identity Servicen ja Primen asentamisesta virtuaalialustalle ja konfiguroinnista nykyiseen kokoonpanoon. Testauksen aloittamista nopeuttaa huomattavasti olemassa olevien verkon päätelaitteiden koostuessa kokonaan Cisco Systemsin laitteista. Käytössä jo valmiiksi ovat Cisco ASA, WLC ja ACS sekä Ciscon tukiasemat, kytkimet ja reitittimet. Testaaminen suoritetaan ISE:n ollessa monitorointitilassa, jolloin erilaisien konfiguraatioiden toimintaa monitoroidaan aivan kun ne olisivat oikeastikin käytössä. Monitorointitilan ollessa päällä käyttäjät voivat käyttää verkkoa aivan normaalisti vaikka autentikointi epäonnistuisikin. Näin minimoidaan häiriöt käyttäjän suuntaan, mutta saadaan silti tieto siitä, miten erilaiset politiikat toimivat verkossa. Tämä onkin yksi ISE:n suurimmista vahvuuksista.

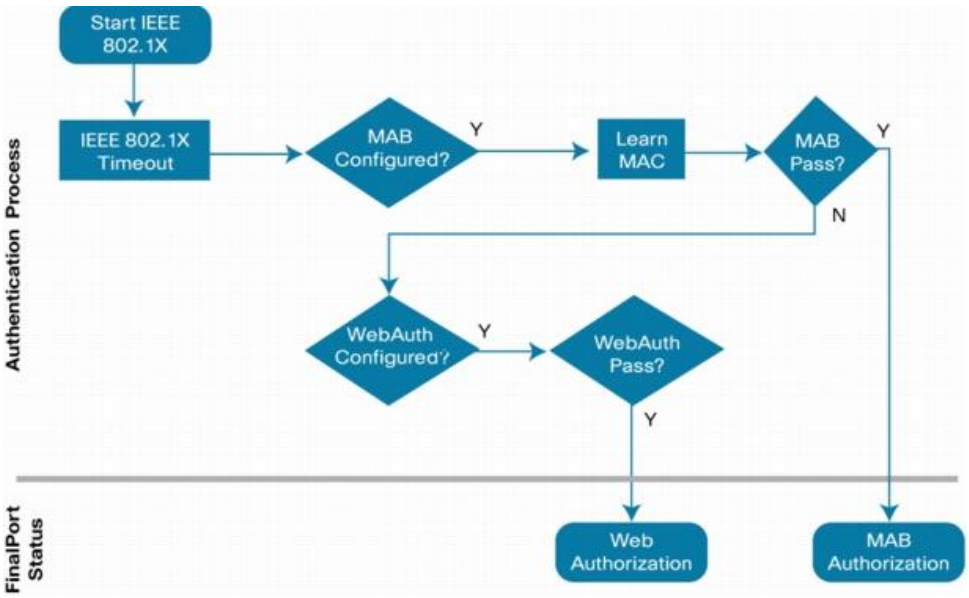
6.2 Käytössä olevat ja testattavat tunnistautumismenetelmät

6.2.1 Testattavat 802.1X-tunnistautumismenetelmät

Uudessa ISE:n kautta tunnistautumisessa tullaan testaamaan EAP-TLS, jossa sekä palvelimelle, että työasemalle asennetaan sertifikaatit. Myös PEAP testataan, tässä sertifikaatti on vain palvelimella ja metodina EAP-MS-CHAPv2. Molemmat tavat tullaan testaamaan sekä Windows 7-, että XP-ympäristöissä, niin langattomilla kuin langallisillakin työasemilla. Supplikanteista tullaan testaamaan molempien Windowssien natiiveja sekä Ciscon Anyconnectia.

6.2.2 MAC Authentication Bypass eli MAB

Laitteille, jotka eivät tue 802.1X-protokollaa on mahdollista konfiguroida MAB eli MAC authentication bypass. Tämä tarkoittaa sitä, että ISE:n tietokantaan lisätään niiden laitteiden MAC-osoitteet joiden tulee päästä verkkoon, mutta mille ei pystytä 802.1X:ää konfiguroimaan. ISE:n profiloinniksi kutsuttu ominaisuus tuo MAB:iin lisää tietoturvaa.

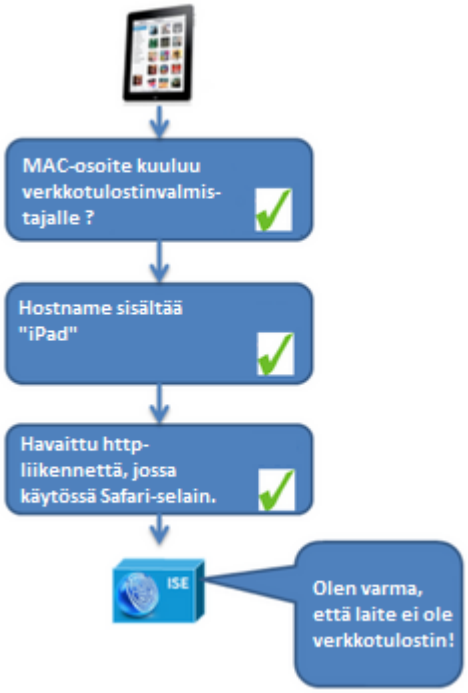


Kuva 34. MAB autentikointiprosessi.

MAB-tietokannan luonti käsin kaikista 802.1X:ää tukemattomista laitteista tuntuu kohtuuttomalle KHSHP:n kokoisessa laitoksessa, sillä esimerkiksi jo verkkotulostimia on satoja. Onneksi MAB-tietokannan laadinta voidaan suorittaa ISE:llä automatisoidusti profiloinnin avulla. ISE:ltä valitaan käyttöön tietty määrä probeja, joille voidaan konfiguroida mahdollisuus tutkia protokollia kuten NetFlow, DHCP, DHCP SPAN, HTTP, Radius, DNS ja muutama erilainen SNMP TRAP/Query. Sensoreina toimivat ISE:en määritetyt kytkimet tai tukiasemat, jotka toimittavat tutkittavan datan probeille. Tämän datan perusteella ISE profiloi laitteita ja näin saadaan esimerkiksi verkkotulostimista automaattinen lista. Täydellistä listaa ei automaattisesti varmaankaan saada, mutta tämä nopeuttaa huomattavasti sen laadintaa.

Profilointia voidaan toki käyttää muuhunkin kuin pelkästään 802.1X:ää tukemattomien laitteiden etsintään. Koska profilointia voidaan suorittaa verkossa jatkuvasti, voidaan esimerkiksi spoofattua MAC-osoitetta käyttävä laite saada selville. Jos joku koittaa tunkeutua sairaalan suojattuun verkkoon käyttämällä vaikkapa verkkotulostimesta anastettua MAC-osoitetta liitettynä iPadiin, saattaa henkilö aluksi päästä MAB:n kautta tulostimelle määriteltyyn verkkoalueeseen. Probet selvittävät kuitenkin nopeasti, että kyseinen laite ei ole verkkotulostin ja laite pakotetaan autenti-

koitumaan normaalisti. Jos tämän MAC-osoitteen omaava tulostin on sidottu käyttämään vain tietyn autentikaattorin tiettyä LAN-porttia, ei tunkeutuja pääsisi näinkään pitkälle.



Kuva 35. Profiloinnilla voidaan nostaa MAB:n tietoturvaa.

6.2.3 WEB-tunnistautuminen

Asiakasverkkoon tullaan ohjaamaan kaikki laitteet, jotka eivät ole MAB-tietokannassa eivätkä kuulu sairaalan hallinnoimien työasemien joukkoon. Kun laitetta ei tunnisteta se ohjataan automaattisesti http-sivulle, jossa käyttäjälle tuotetaan tunnus ja salasana, jotka ovat käytössä ennalta määrätyn ajan. Tällä päästään helposti eroon turhaa verkossa roikkuvista mobiililaitteista.

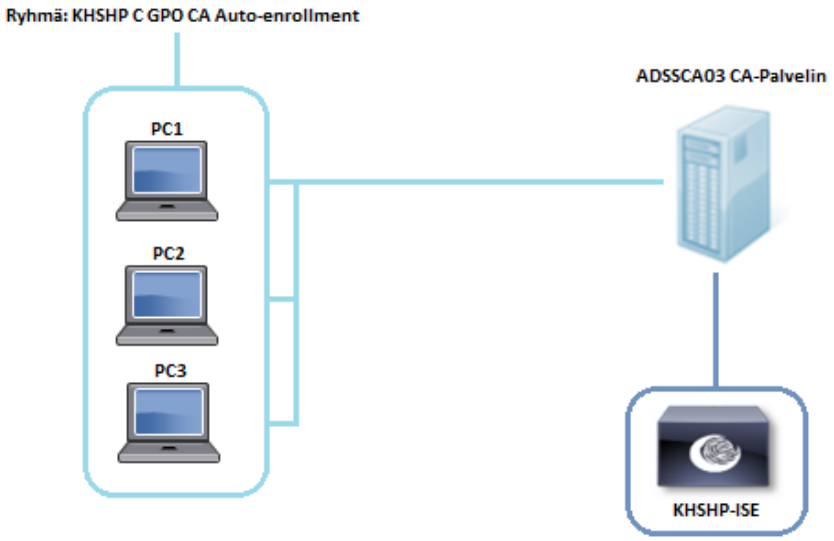
WEB-tunnistautumista ei päästy työn aikana testaamaan, sillä sairaalalla on käytössä noin kymmenen tukiasemaa, jotka eivät tue Wireless Lan Controllerin verisiota, jolla WEB-tunnistautumistumisportaali oli tarkoitus rakentaa ja testata. Tämä on kuitenkin tulevaisuudessa varmasti mahdollista, heti kun tukiasemakanta saadaan kokonaan uusittua.

6.3 Sertifikaattipalvelin ja PK-Infrastruktuuri

802.1X-testausta varten pystytettiin sairaalalle oma sertifikaattipalvelin XXXXXX. Palvelimeksi tuli Windows Server 2008 R2 Enterprise. Palvelimelle määriteltiin “Active Directory Certificate Services” –rooli Enter-

prise Root CA, uusi yksitasoinen Enterprise Root CA sekä KHSHP Root-Issuing CA. Root-sertifikaatti määriteltiin olemaan voimassa XX vuotta. Palvelimelle asennettiin myös ”Web Enrollment”-palvelu.

Työasemasertifikaatin jakelua varten luotiin sertifikaatti template ”KHSHP Workstat Authentication”. Tähän templeittiin asetettiin Auto-Enrollment luvat ”KHSHP GPO Auto-enrollment”-ryhmälle ja AD:lle luotiin uusi politiikka ”KHSHP Auto-Enrollment”, jolla Auto-Enrollment asetukset jaellaan. Jotta sertifikaatti lähetetään työasemalle, tulee työaseman kuulua uuteen ”KHSHP GPO Auto-Enrollment”-ryhmään. Kun työasema lisätään tähän ryhmään myönnetään sille automaattisesti uudelleenkäynnistyksen jälkeen sertifikaatti, joka on voimassa neljä vuotta. Neljän vuoden raja on sama kuin työasemien liisausaika.



Kuva 36. CA-Infrastruktuuri.

ISE:n sertifikaattia varten luotiin sertifikaatti template ”KHSHP Web Server RADIUS”. Tähän templeittiin asetettiin enroll-luvitukset ”KHSHP Enroll Admins” ryhmälle. Palvelinsertifikaatti on voimassa kahdeksan vuotta. Jotta sertifikaatti saatiin ISE:lle tuli ”KHSHP Enroll Admins”-ryhmään kuuluvan anoa se http://xxxxxxxxxxxx -osoitteesta ja siirtää sitten ISE:n kantaan.

Kuva 37. Identity Services Enginelle asennettu sertifikaatti.

6.4 Identiteettilähteet

ISE:n autentikointipoliitkoiden rakentamisessa käytetään hyväksi erilaisia identiteettilähteitä. Sairaalalla identiteettilähteenä voidaan käyttää AD:n kantoja jossa on ylläpidettynä valmiiksi työntekijät ja työasemien nimet.

Näin jokainen sairaalan hallinnoima kone voitaisiin tunnistaa ilman sertifikaattiakin. Sertifikaatin käyttö on silti suositeltavaa, sillä se lisää tietoturvaa runsaasti. AD:ssa voidaan kuitenkin erotella esimerkiksi kannettavat tietokoneet pöytäkoneista ja käyttäjäryhmät toisistaan. Kaikki tämä kuitenkin edellyttää Active Directoryn tarkkaa ylläpitoa ja päivittämistä.

Kuva 38. KHSHP:n Active Directory ulkoisena identiteettilähteenä ISE:ssä.

6.5 Identity Service Enginen pystytys

Identity Service Engine-palvelin pystytettiin testaamisen ajaksi virtuaalialustalle Fujitsun Konalan konesaliin. Oikeaan käyttöön otettaessa on suositeltavaa asentaa ISE fyysisesti samaan paikkaan valvottavan verkon kanssa, eikä 100 kilometrin päähän. Autentikointien ja valvonnan tulee olla reaaliaikaista ja pitkän matkan päässä sijaitseva konesali sekä jaetut 100Mt/s linjat eivät ole yhtä luotettavia, kuin sairaalan oma konesali yhdistettynä 10Gt kuituverkkoon.

6.6 Wireless Lan Controllerin liittäminen Identity Services Engineen

Jotta langattomat laitteet saadaan myös 802.1X:n piiriin tulee WLC:lle konfiguroida oma SSID tätä varten. WLC tulee myös liittää ISE:n verkkolaitteiden kantaan.

WLC:lle luodaan ensiksi WLAN ID ”khshp1x”. WPA2 encryptauksena käytetään AES:a ja autentikointiin 802.1X:ää. Käytettäväksi RADIUS-palvelimeksi määritetään autentikointia varten ISE.

Kuva 39. 802.1X:ssä käytettävän SSID:n kofiguraatio WLC:llä.

Lopuksi luodaan AP-Group, johon lisätään kaikki ne Access Pointit joiden halutaan tukevan 802.1X:ää. Tähän ryhmään kuuluvat tukiasemat sisältävät vain khshp1x ja asiakasverkko SSID:t. Näin voidaan kontrolloida millä langattoman verkon alueilla 802.1X:ää testausvaiheessa tuetaan.

6.7 Kytkinten eli autentikaattoreiden konfigurointi

Jokainen kytkin joka halutaan toimivaksi 802.1X autentikaattorina on konfiguroitava tätä tehtävää varten. Seuraavassa yleisesti kytkimiin, sekä jokaiseen autentikoivaan porttiin tehty konfiguraatio.

```
802.1x Interface configuraatio:

interface GigabitEthernet0/41
 switchport access vlan xx
 switchport mode access
 authentication host-mode multi-auth
 authentication open
 authentication port-control auto
 authentication timer restart 0
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
 dot1x max-reauth-req 1
 storm-control broadcast level 1.00
 storm-control multicast level 1.00
 spanning-tree portfast
!

Yleisesti kytkimelle:

authentication mac-move permit
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
aaa authentication dot1x default group radius
dot1x system-auth-control
radius-server dead-criteria time 5 tries 3
radius-server host 111.111.111.111 auth-port 1111 acct-port
1111 key 7 XXXXXXXXXXXXXXXXXXXXXXXX
```

6.8 Identity Services Enginen konfigurointi

Yksi koko työn mielenkiintoisimmista ja tärkeimmistä vaiheista on saada ISE konfiguroitua sillä tavalla, että säännöstö vastaa haluttua politiikkaa sairaalalla. Laitteet ja käyttäjät autentikoidaan oikeista paikoista ja ne saavat vaaditun autorisoinnin eli saavat käyttöönsä tarvittavat verkkoresurssit.

6.8.1 Autentikaattorien lisääminen Identity Services Engineen

Jotta verkossa voidaan suorittaa 802.1X autentikointia, tulee ISE:lle lisätä autentikaattorit. Kytkimissä tulee olla vähintään käyttöjärjestelmäversio 12.2(55)SE, jotta ne tukisivat 802.1X autentikointia. ISE:ssä autentikaattorit lisätään ”Administration – Network Resources – Network Devices”-kohdan alta.

(http://www.cisco.com/en/US/docs/security/ise/1.1/compatibility/ise_sdt.html#wp55038)

Kuva 40. Autentikaattorin lisääminen Identity Services Engineen.

Autentikaattorista määritellään nimi ja ip-osoite, sekä mihin laiteryhmään se kuuluu. Autentikointi asetuksista tulee määrittää salasana, joka on määritelty sekä ISE:lle, että kytkimille. Kytkimelle autentikointi määritellään seuraavalla komennolla:

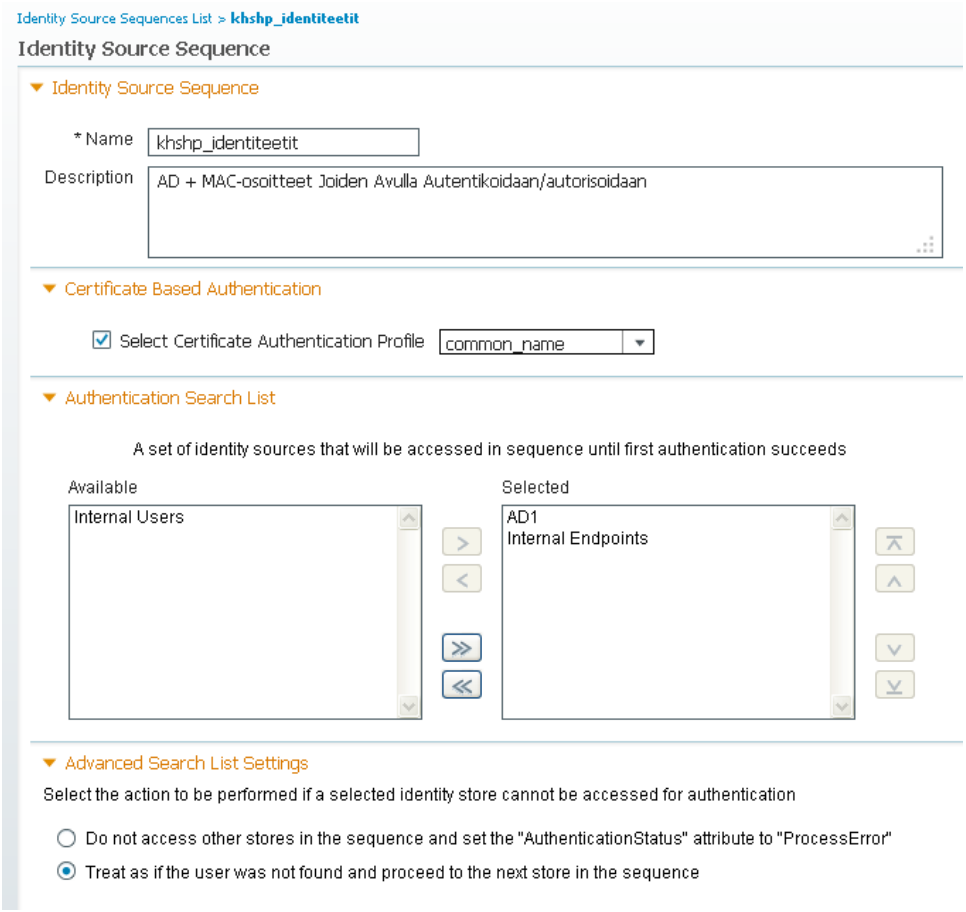
```
radius-server host 172.25.0.248 auth-port 1812 acct-port
1813 key 7 XXXXXXXXXXXXXXXXX
```

Langattomalta puoleta ei tarvise ISE:lle lisätä, kuin WLC. Tämä hoitaa tukiasemien toiminnan autentikaattoreina. Jos 802.1X otettaisiin laajaan käyttöön, tulisi tähän listaan lisätä jokainen sairaalan autentikaattorina toimiva kytkin. Jokaisen kytkimen pitäisi myös kyetä käyttäämään vähintään versiota 12.2(55)SE. Sairaalalla on tällä hetkellä muutama kytkin, jotka eivät tätä tue. Nämä pitää ottaa huomioon ja uusia laajemman käyttöönoton tullessa kyseeseen.

Kuva 41. Identity Service Enginelle lisättyjä autentikaattoreina tomivia verkkolaitteita.

6.8.2 Identiteettilähteiden konfigurointi

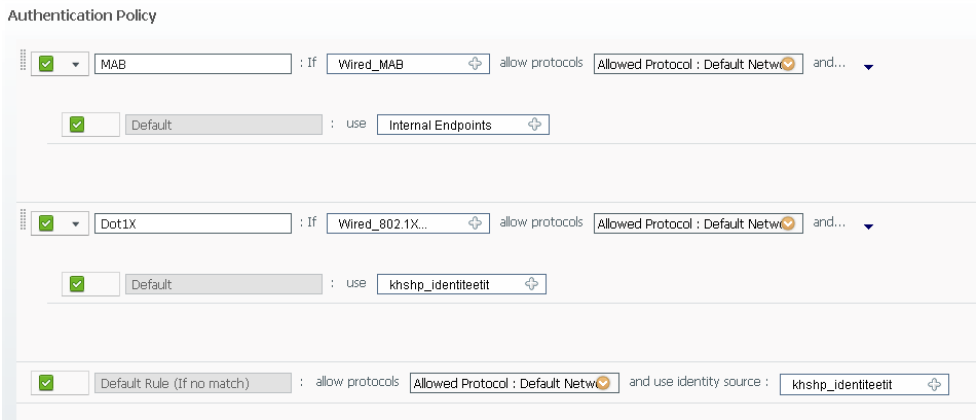
Aluksi ISE:en lisätään jo olemassa oleva identiteettilähde eli sairaalan AD. Tämä tapahtuu lisäämällä ISE samaan domainiin sairaalan AD:n kanssa. Lisäksi konfiguroidaan AD-ryhmät ISE:lle, joita ovat testauksen ajan KHSHPAD/Users/Domain Computers, KHSHPAD/Users/Domain Users ja KHSHPAD/khshp/RYHMAT/KHSHP Kannettavat. Näin saadaan käyttöön henkilötiedot, konetiedot ja vielä eroteltua pöytäkoneet kannettavista tietokoneista. Tämän jälkeen on hyvä luoda sekvenssi identiteettilähteille. Tämä tarkoittaa, että jos laitetta ei löydy AD:sta käydään seuraavaksi läpi ”Internal Endpoints”-lista, joka sisältää MAC-osoitteen avulla 802.1X autentikoinnin ohittavat laitteet.



Kuva 42. ISE identiteettisekvenssi.

6.8.3 Autentikonti politiikka

Autentikointi politiikkassa määritetään protokollat joita ISE sallii käytettävän autentikointiin, sekä ne identiteettilähteet joita autentikoinnissa käytetään.



Kuva 43. KHSHP:n ISE:ssä oleva autentikointi politiikka

Sallituissa protokollissa voidaan määritellä esimerkiksi, että 802.1X:ää käytettäessä vain EAP-TLS on sallittu ja kaikki muu dropataan.

6.8.4 Autorisointi profiilit

Autorisointi profiileilla erotetaan autentikoinnin tuloksena laitteet ja käyttäjät erilaisiin ryhmiin. Testivaiheessa käyttöön otetaan PC-KHSHP, LAPTOP-KHSHP, MAB ja BYOD. BYOD tulee sanoista ”Bring Your Own Device” ja tätä käytetään kun käyttäjä tunnistetaan, mutta laitetta ei löydy sairaalan tietokannasta tai sillä ole vaadittua sertifikaattia.

KHSHP-PC-profiiliin kuulvat ne PC:t joita sairaalan IT-yksikkö ylläpitää. Kun autentikointi mahdollistaa laitteen liittämisen tähän autorisointi profiiliin saa kone verkkoon ”ACCESS_ACCEPT”-tyypin pääsyn eli rajoittamattoman verkkokäytön suojatun verkon puolelta.

KHSHP-LAPTOP-profiiliin kuuluvat sairaalan kannettavat tietokoneet. Niille annetaan myös ”ACCESS_ACCEPT” ja täten täysi pääsy verkkoon.

BYOD-profiiliin tippuvat laitteet tullaan tulevaisuudessa ohjaamaan asiakasverkkoon. BYOD:een kuuluvat ne laitteet joita ei löydy AD:sta, mutta käyttäjä kuitenkin autentikoidaan. Tällaiset tapaukset voidaan esimerkiksi siirtää asiakasverkkoon gold-statuksella, jolloin kaistaa varataan enemmän kuin perus käyttäjille. BYOD-käyttäjille voidaan myös rakentaa oma pääsy ulkoverkkoon, joka olisi erillään sekä asiakasverkosta, että sairaalan sisäverkosta. Posturen ollessa käytössä voidaan harkita jopa BYOD-laitteiden osittaista päästämistä sisäverkkoon. Tällöin käyttäjän koneesta tarkastettaisiin Windows-päivitykset ja virusturvan ajantasaisuus ennen verkkoon päästämistä. Testausta tehdessä ei WLC:n versio vielä taivu webauthiin eikä sitä voida päivittää, sillä käytössä on vielä vajaa 20 kappaletta tukiasemia jotka eivät enää tue WLC:n uutta versiota. Testauksen aikana kuitenkin tarkastellaan kuinka laitteet jotka eivät löydy identiteettikannoista ohjataan oikeaan lokeroonsa eli saavat BYOD-profiilin.

Laitteet jotka eivät osaa 802.1X:ää ja kuitenkin tarvitsevat sairaalan verkkoresursseja toimiakseen liitetään MAB-profiiliin. ISE pitää sisällään listaa, johon voidaan lisätä MAC-osotteita halutuista laitteista. Kun ISE havaitsee verkkoon pyrkivän laitteen, jonka MAC-osoite löytyy ISE:n Internal Endpoints-listalta ohitetaan 802.1X-autentikointi ja laite päästetään suojattuun sisäverkkoon.

6.8.5 Autorisointi politiikka

Kun profiilit on luotu, voidaan siirtyä tekemään autorisointi politiikkaa. Tässä määritellään ehdot ja säännöt joiden avulla laiteille annetaan tietyt halutut oikeudet.

Kuva 44. KHSHP:n autorisointi politiikka.

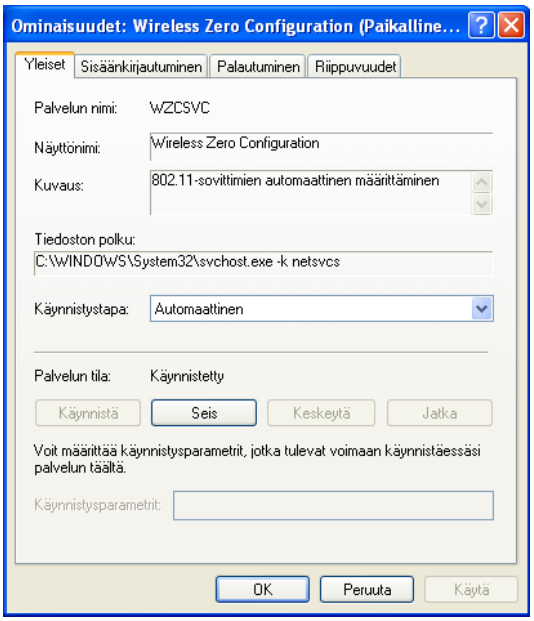
ISE käy säännöt läpi ylhäältä alas. Ensimmäisenä tarkastetaan kuuluuko laite kannettaviin tietokoneisiin eli löytyykö laitteen nimi AD:n läppäriryhmästä ja jos löytyy siirretään laite LAPTOP-KHSHP-profiiliin. Jos ei, siirrytään seuraavaan eli tarkastetaan kuuluuko laite työasemiin. Jos laitetta ei löydy edellisistä ryhmistä, tarkastetaan kuuluuko laitteen käyttäjä sairaalan henkilökuntaan ja tällöin saisi BYOD-profiilin. Jos mikään edellisistä ei ole pitänyt paikkaansa tarkastetaan Mac Authentication Bypass-lista. Koska kyseessä on testivaihe, on viimeisenä sääntönä ”Default – PermitAccess” eli vaikka konetta tai käyttäjää ei löydy mistään, saa verkkoon silti täyden pääsyn. Tämän takia käyttäjien toiminta ei häiriinny, mutta voidaan silti tarkkailla ja hienosäätää konfiguroraatioita niin, että käyttöön otettaessa kaikki toimisi kunnolla.

7 SUPPLIKANTTIEN KONFIGUROINTI JA TESTAUS

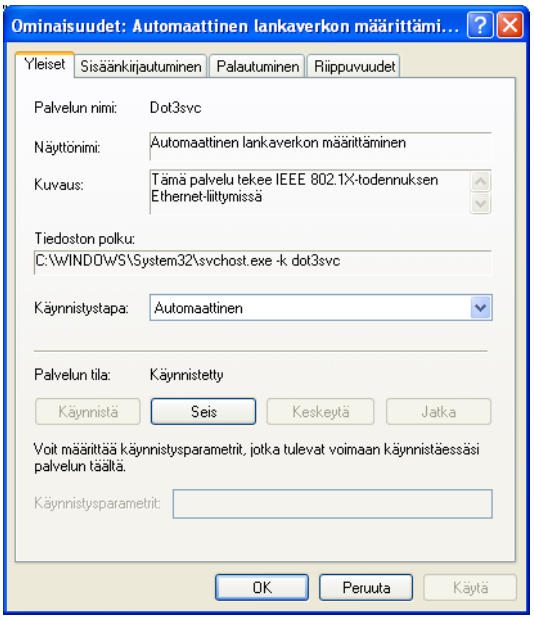
802.1X-testauksen aikana käydään käyttöjärjestelmistä läpi sekä Windows XP, joka on vielä suurimmassa osassa sairaalan työasemia käytössä, että Windows 7, joka tulee olemaan pääasiallinen käyttöjärjestelmä tulevaisuudessa. Molemmilla käyttöjärjestelmillä testataan langaton ja langallinen yhteys. Supplikantteina käytetään XP:n ja 7:n omia windowsien mukana tulleita supplikantteja, sekä Ciscon tarjoamaa ilmaista Anyconnect-supplikanttia. Protokollina EAP-PEAP ja EAP-TLS. Lopuksi testataan Mac Authentication Bypass muutamilla eri laitteilla, jotka eivät tue 802.1X autentikointia. Huomionarvoista on, että opinnäytetyön aikarajat eivät venyneet pidempiaikaiseen testaukseen. Supplikanteista voitiin testata vain yhteensopivuus ja eri autentikointimuotojen toimivuus eri käyttöjärjestelmillä ja konfiguraatioilla. Jos ISE ja 802.1X autentikointi aiotaan ottaa tuotantokäyttöön, tulee autentikointia ja laitteiden pääsynhallintaa vielä testata laajemmalti.

7.1 Windows XP

Windows XP:ssä langaton 802.1X supplikantti on palvelu nimeltään Wireless Zero Config. XP Service Pack 3 myötä lankaverkon 802.1X:ää säädellään DOT3SVC-palvelulla, joka on suomeksi ”Automaattinen lankaverkon määrittäminen”. Molemmat palvelut tulee määrittää automaattisesti käynnistyviksi. Nämä supplikantit tukevat sekä kone- että käyttäjäautentikointia sekä EAP-tyyppejä PEAP-MSCHAPv2, PEAP-TLS, TLS ja MD5. (http://support.microsoft.com/kb/950725)

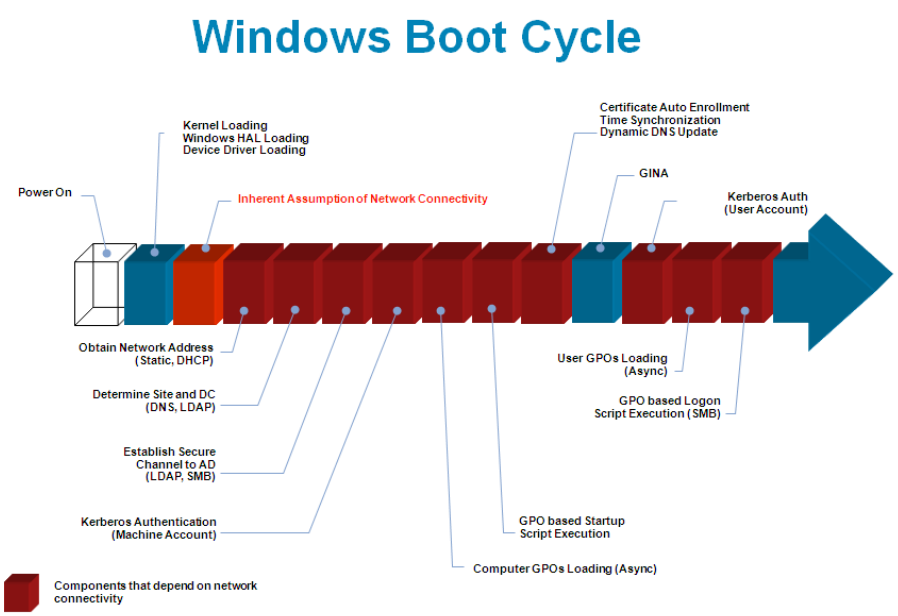


Kuva 45. Win XP Wireless Zero Configuration-palvelu.



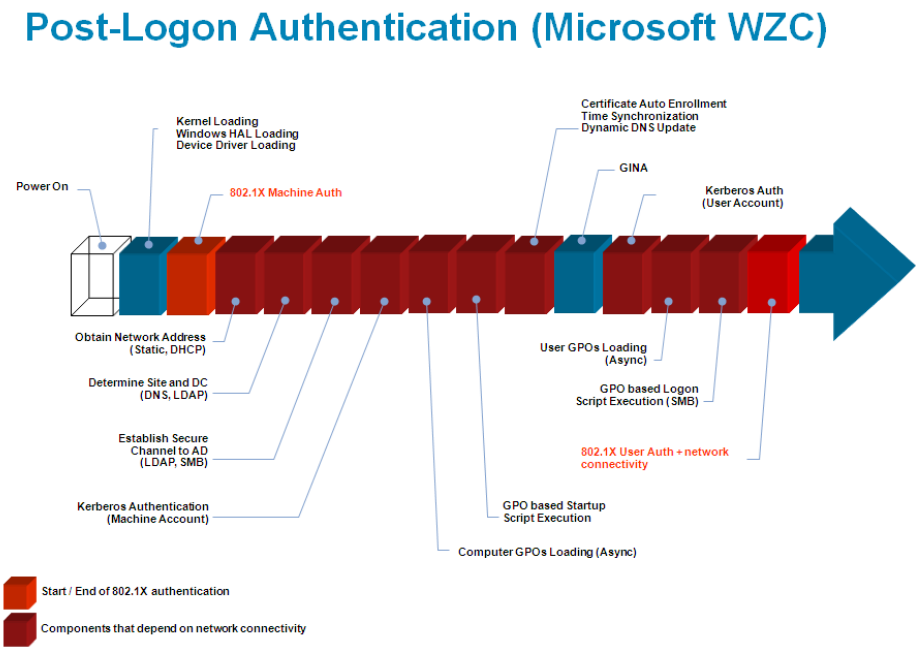
Kuva 46. Win XP Automaattinen lankaverkon määrittäminen-palvelu.

Windows koneisiin olisi syytä saada koneautentikointi toimimaan, sillä muutoin yhteyttä verkkoon ennen käyttäjän kirjautumista ei saada. Koneautentikointi tapahtuu boottauksen yhteydessä ja tällöin käyttäjän koneelle saadaan oikeat ryhmäkäytännöt AD:lta.



Kuva 47. Windows XP:n Boot Cycle

Kuvasta 47 nähdään, että ennen käyttäjäautentikointia XP-kone tarvitsee jo verkkoresursseja ladatessaan eri GPO:t domain controllerilta. Koska sairaalalla monet GPO:t on osoitettu konekohtaisesti, tulee verkkoyhteyden oltava kunnossa ennen kirjautumista. Toisin sanoen, jos supplikantilla ei saada koneautentikointia järkevästi toimimaan sitä ei voida sairaalalla käyttää. (IEEE 802.1X/NAC Technology & Solution TOI, Mitsunori Sagae 2007)



Kuva 48. käyttäjäautentikointi Win XP natiivilla supplikantilla.

Microsoftin omalla supplikantilla 802.1X käyttäjäautentikointi tapahtuu auttamattomasti myöhässä ryhmäkäytäntöjen lataamisen kannalta. Kuvasta

8 nähdään hyvin miten 802.1X koneautentikointi ja käyttäjäautentikointi eroavat ajallisesti toisistaan. (IEEE 802.1X/NAC Technology & Solution TOI, Mitsunori Sagae 2007)

7.1.1 Win XP LAN 802.1X EAP-PEAP Microsoftin supplikantilla

KHSHP:ssa on vielä laajasti käytössä Windows XP SP3. Jotta tässä Windows versiossa saadaan natiivi supplikantti toimimaan täytyy rekisteriin, lähiverkkoprofiiliin ja itse supplikanttiin tehdä muutamia muutoksia.

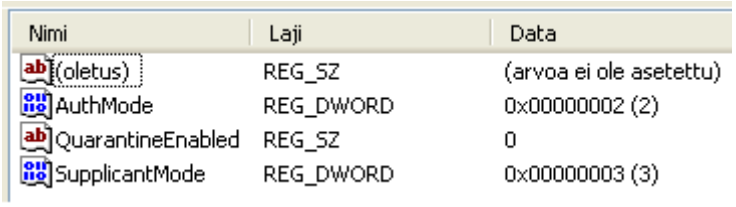
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EAPOL\Parameters \General\Global\ -alle tulee lisätä kaksi DWORD-arvoa. AuthMode ja SupplicantMode. AuthMode voi saada arvot 0-2. (http://support.microsoft.com/kb/309448/en-us)

```
Arvo        Selitys

0           Default Windows XP authentication
1           Always perform user authentication
2           Perform machine authentication only
```

SupplicantMode voi saada arvot 0-3

```
Arvo        Selitys

0           Disable IEEE 802.1X auth operation
1           Prevent EAPOL start and EAPOL log off packets
2           Include learning to determine when to initiate 3
            the transmission of EAPOL packets.
3           Compliant with IEEE 802.1X authentication speci-
            fication.
```

AuthModeksi valitaan arvo “2” ja SupplicantModeksi arvo “3”.

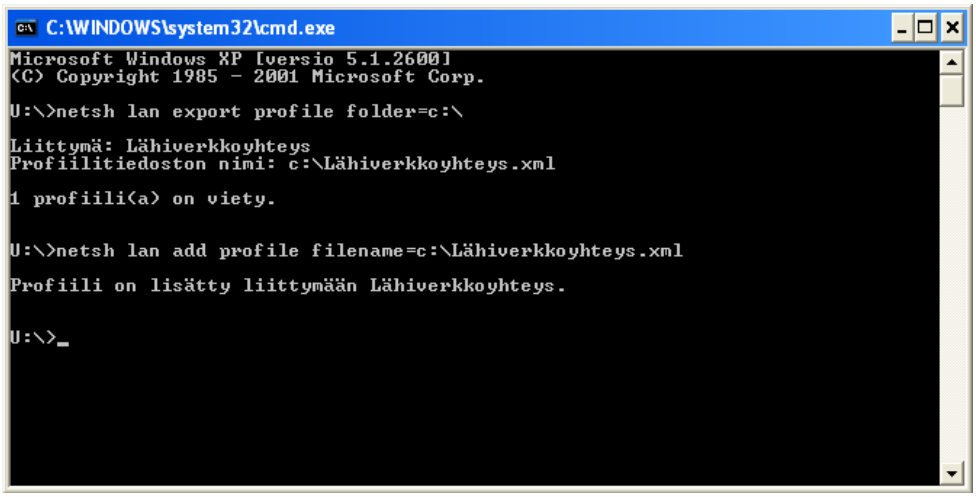


Kuva 49. Windows XP:n rekisteriin lisättävät DWORD –arvot.

Seuraavaksi eksportataan langallisen yhteyden asetukset XML-tiedostoksi, jotta sitä voidaan muokata. XML-tiedostoon lisätään

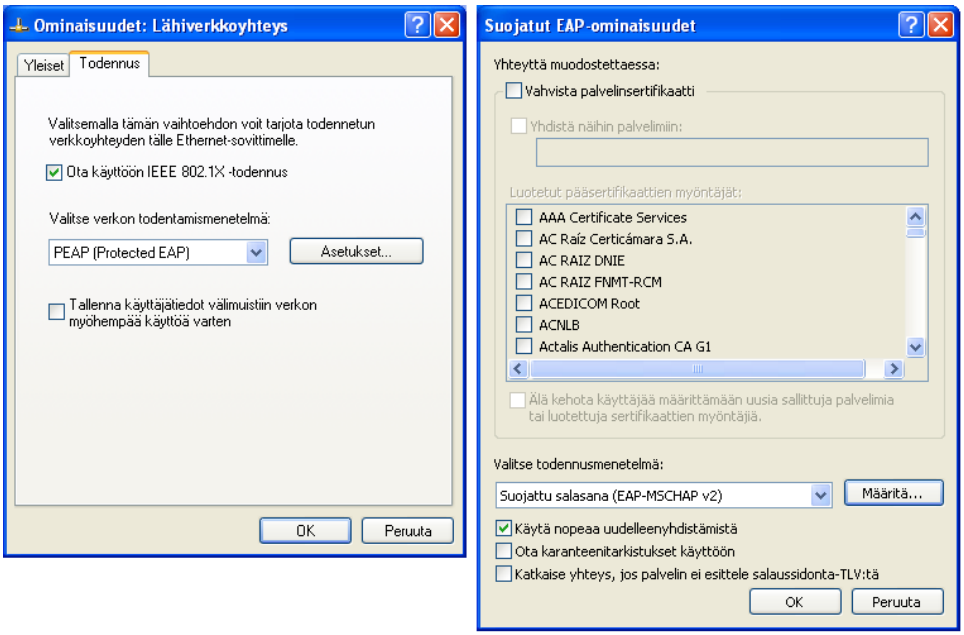
```
<AuthMode>machine</AuthMode>
```

Tämän jälkeen XML tallennetaan ja lisätään takaisin käytettävään lähiverkkoyhteyteen. (http://support.microsoft.com/kb/929847)



Kuva 50. Lähiverkkoprofiilin muokkaus tukemaan ainoastaan koneautentikointia.

Lopuksi konfiguroidaan itse supplikantti. Jotta lähiverkkoyhteyteen saadaan näkyviin ”Todennus”-välilehti tulee palvelun ”Automaattinen lankaverkon määrittäminen” olla käynnissä. ”Todennus”-välilehdeltä valitaan käyttöön IEEE 802.1X ja valitaan todentamismenetelmäksi PEAP (Protected EAP). PEAP-määrityksistä todennusmenetelmäksi valitaan EAP-MSCHAPv2.



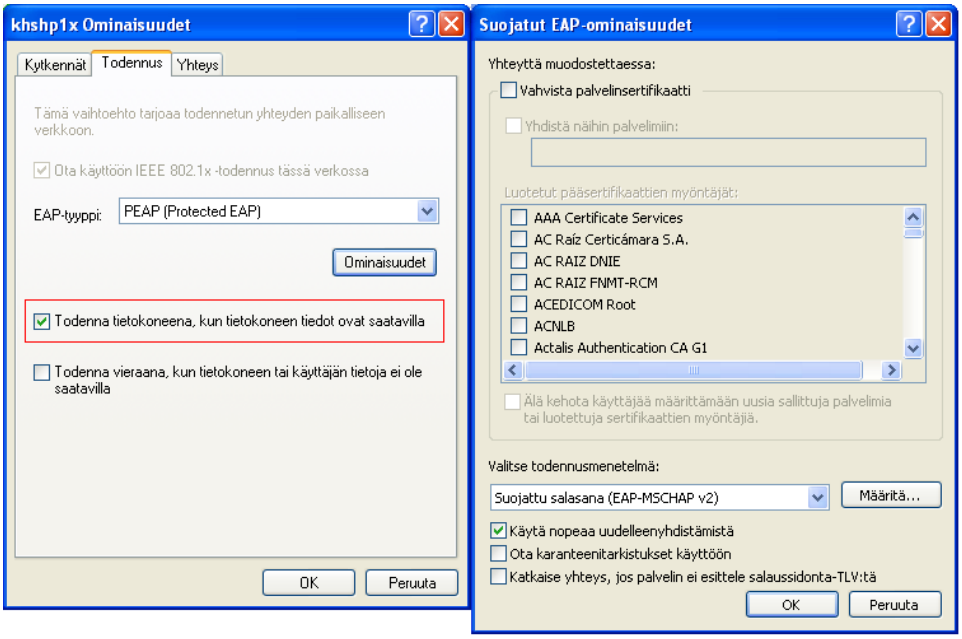
Kuva 51. Win XP SP3 802.1X natiivin LAN-supplikantin PEAP-konfigurointi.

Kun kaikki nämä asettelut on tehty, voidaan kone liittää 802.1X konfiguroituun kytkinporttiin ja tarkastella ISE:n liveautentikoinneista miten kone autentikoituu. Liitteestä 1 voimme nähdä, että laite on autentikoitunut onnistuneesti käyttäen protokollana EAP-MSCHAPv2:sta, metodina dot1x:ää sekä tippunut oikeaan autorisointiprofiiliin LAPTOP-KHSHP (käytössä kannettava tietokone liitettynä lankaverkkoon). Koneen käynnistyessä ISE:n Live Authentications-ikkunasta pystytään seuraamaan, että autorisointi sairaalan suojattuun verkkoon tapahtuu windowsin määrittäes-

sä verkkoyhteyksiä ennen kirjautumisikkunaa. Tästä voimme päätellä kaiken toimivan oikein.

7.1.2 Win XP WLAN 802.1X EAP-PEAP Microsoftin supplikantilla

Jotta langattoman verkon puolelle saadaan 802.1X-autentikointi toimimaan tulee rekisteriin tehdä samat muutokset, kuin lähiverkonkin kohdalla. WLC:lle on luotu oma SSID 802.1X-todennusta varten. Supplikantille määritellään WPA2/AES ja EAP-tyypiksi PEAP. Langattoman verkon natiivissa supplikantissa on valmiiksi kohta ”Todenna tietokoneena, kun tietokoneen tiedot ovat saatavilla” ja tämän vuoksi ei tarvitse muokata tuota profiilista eksportattua XML:ää kuten langallisen lähiverkon puolella. (http://technet.microsoft.com/en-us/network/dd727529.aspx#EWKAC)

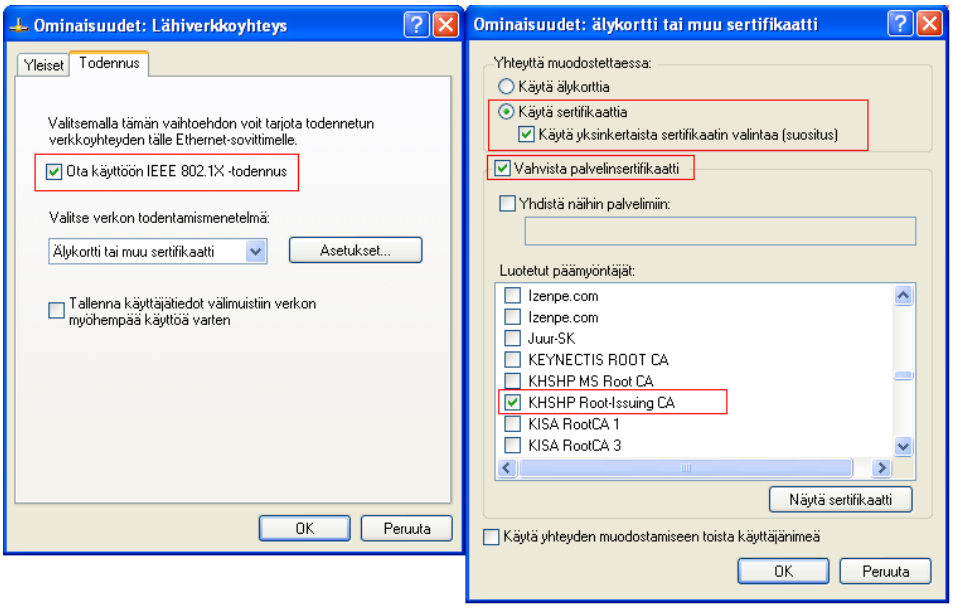


Kuva 52. Win XP SP3 802.1X natiivin WLAN-supplikantin PEAP-konfigurointi.

Konfiguroinnin päätteeksi voidaan kone käynnistää uudelleen. Jälleen ISE:n reaaliaikaisia autentikointeja seuraamalla voidaan todeta, että koneautentikointi toimii hienosti heti Windowssin ladatessa verkkokokoonpanot (liite 2). Levyjaot ja GPO:t tulevat moitteettomasti käyttöön.

7.1.3 Win XP LAN 802.1X EAP-TLS Microsoftin supplikantilla

EAP-TLS:ää käytettäessä on sekä työasemalla, että palvelimella oltava sertifikaatti. Konfiguraatio itse työasemalle ei ole sen monimutkaisempi, kuin PEAP:ssa. Työasemien tulee olla ”KHSHP GPO Auto-enrollment”-ryhmässä, jotta sertifikaattijakelu tulee perille.

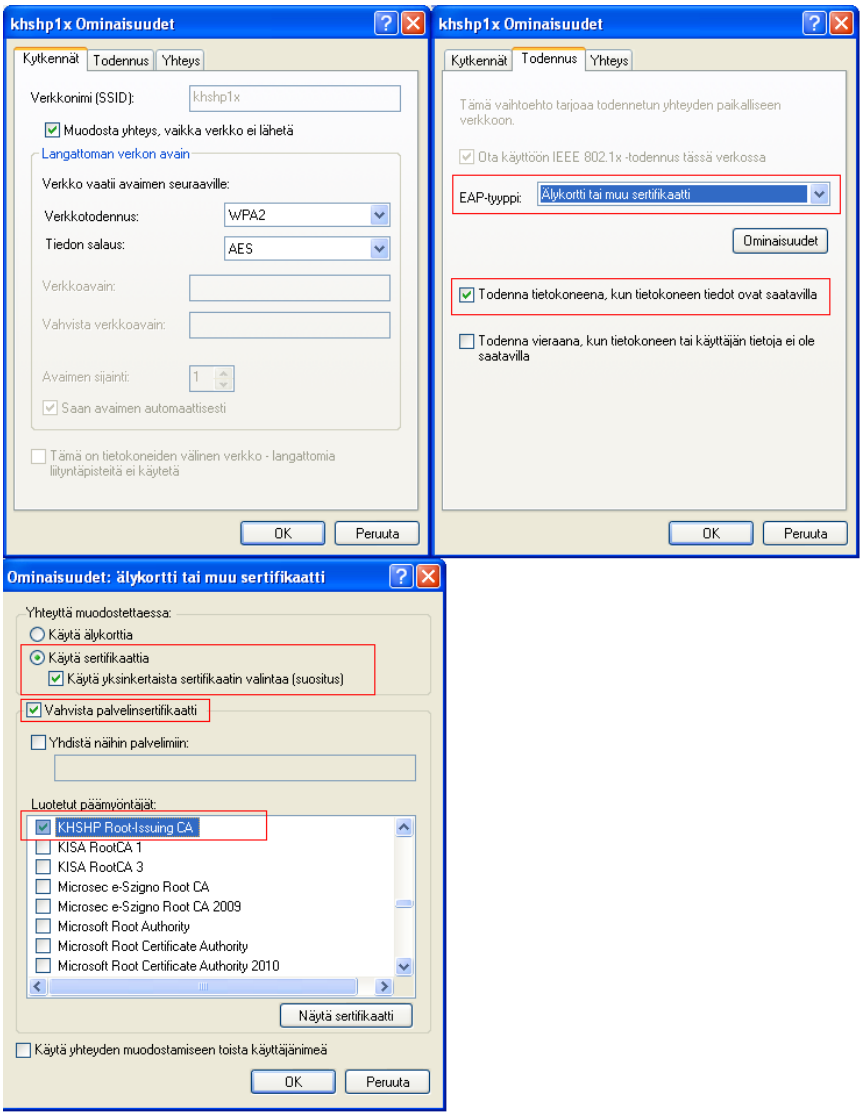


Kuva 53. Win XP SP3 802.1X natiivin LAN-supplikantin EAP-TLS-konfigurointi.

Kunhan ”automaattinen lankaverkon määrittäminen”-palvelu on käynnissä, voidaan ”Todennus”-välilehdeltä ottaa käyttöön 802.1X ja valita sertifikaatti todennusmenetelmäksi. Asetuksista valitaan sertifikaatin käyttö sekä palvelinsertifikaatin vahvistus. Liitteestä 3 näkyy laitteen onnistunut autententikointi ISE:llä.

7.1.4 Win XP WLAN 802.1X EAP-TLS Microsoftin supplikantilla

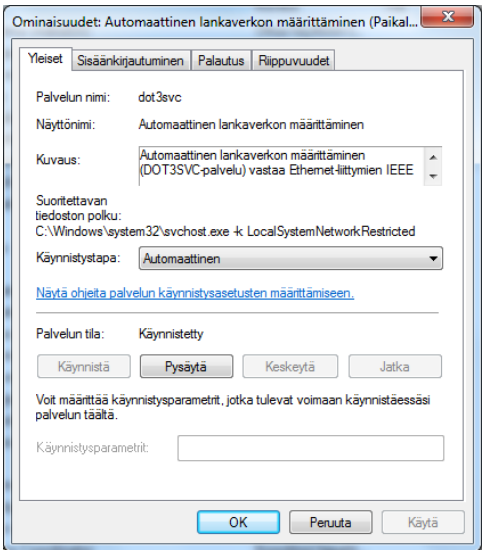
Langattoman verkon konfigurointi tapahtuu langattoman verkkoyhteyden ”Ensisijaiset verkot”-ikkunan kautta. Valitaan khshp1x SSID muokattavaksi EAP-TLS asetteluja varten. Verkkotodennus ja tiedon salaus samat kuin PEAP:ssa, todennuksesta valitaan EAP-tyypiksi ”Älykortti tai sertifikaatti”, sekä valitaan ”Todenna tietokoneena”. Sertifikaatin ominaisuuksista valitaan ”Yksinkertainen sertifikaatin valinta” ja ”Varmista palvelinvarmenne”, sekä valitaan päämyöntäjäksi KHSHP:n juuripalvelin. Liitteestä 4 voimme tarkastella onnistuneen autentikoinnin parametreja ISE:llä.



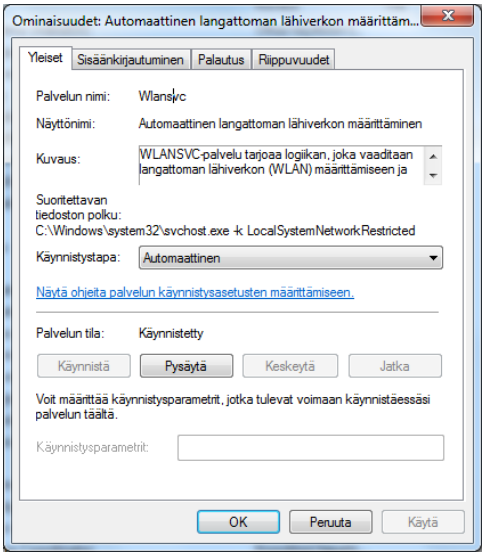
Kuva 54. Win XP SP3 802.1X natiivin WLAN-supplikantin EAP-TLS-konfigurointi.

7.2 Windows 7

Myös Windows 7 pitää sisällään erilliset natiivit supplikantit sekä langalliselle, että langattomalle lähiverkolle. LAN-verkon puolella 802.1X supplikantti on palvelu nimeltään ”Automaattinen lankaverkon määrittäminen” eli DOT3SVC. WLAN-verkon puolella se on ”Automaattinen langattoman lähiverkon määrittäminen” eli WLANSVC. DOT3SVC vastaa Ethernet-liittymien IEEE 802.1X todennuksesta, se ei vaikuta niihin lankaverkon yhteyksiin, jotka eivät tue 802.1X:ää. WLANSVC hoitaa saman langattoman verkon puolella. (http://windows.microsoft.com/en-sg/windows-vista/enable-802-1x-authentication)



Kuva 55. Windows 7 natiivi LAN-supplikantti.

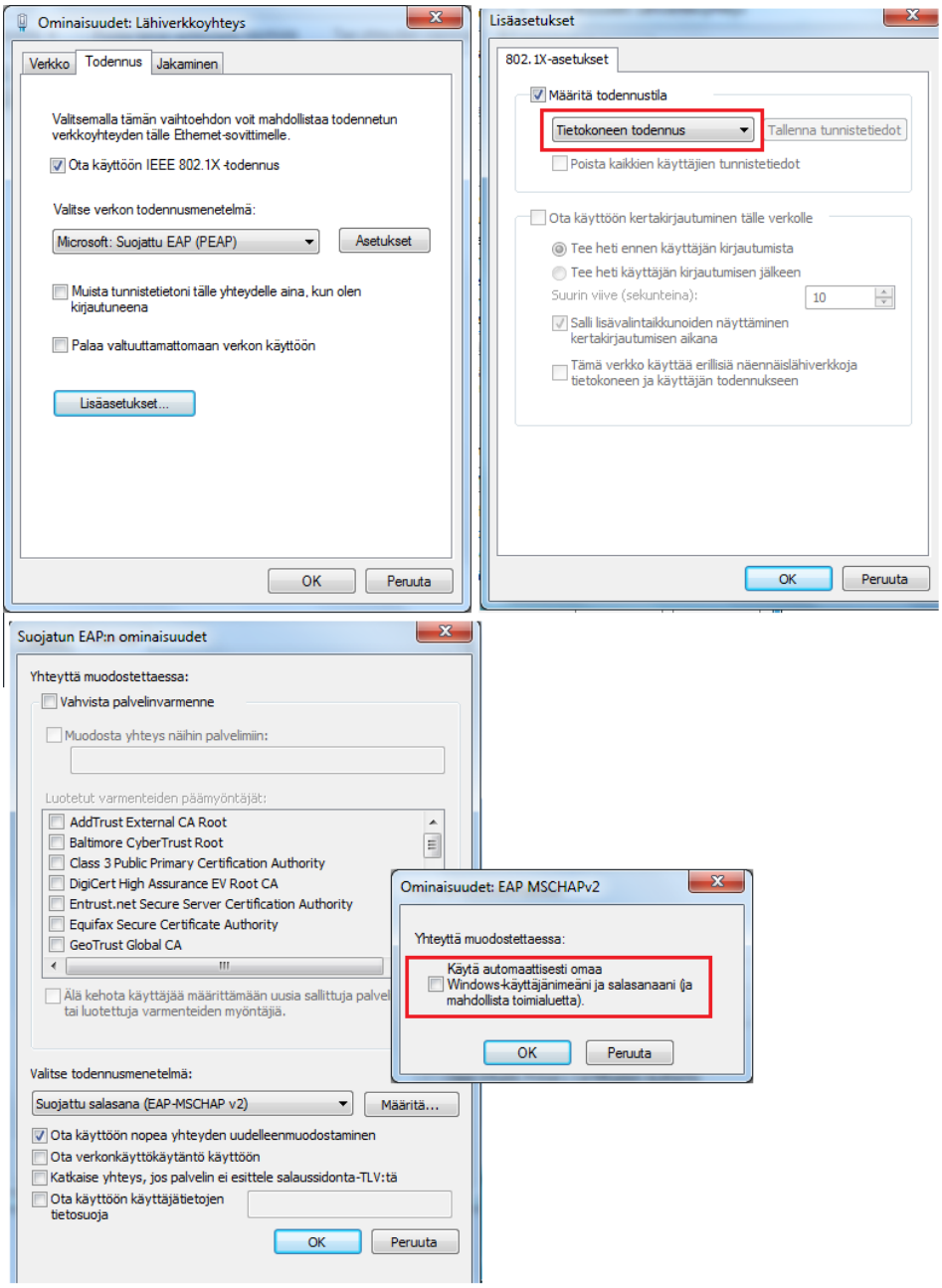


Kuva 56. Windows 7 natiivi WLAN-supplikantti.

Windows 7:n supplikantit tukevat laajempaa kirjoa 802.1X-todennusmenetelmiä kuin Windows XP:ssä. Windows 7 tarjoaa tuen seuraaville menetelmille: EAP-PEAP, Cisco LEAP, Cisco PEAP, Cisco EAP-FAST, Intel EAP-SIM, Intel EAP-TTLS ja Intel EAP-AKA. Testaukseen valitaan kuitenkin vain EAP-PEAP ja EAP-TLS.

7.2.1 Windows 7 LAN 802.1X EAP-PEAP Microsoftin supplikantilla

Windows 7:ssä ei tarvitse rekisteriin tehdä muutoksia kuten Windows XP:ssä. Riittää kun ”Todennus”-välilehdeltä ottaa IEEE 802.1X todennuksen käyttöön ja valitsee halutun todennusmenetelmän. Huomionarvoista on muistaa lisäasetuksista määrittää käyttöön ”Tietokoneen todennus”, sekä EAP-MSCHAPv2-ominaisuuksista ottaa käyttäjätunnistuksen pois päältä yhteyttä muodostettaessa.

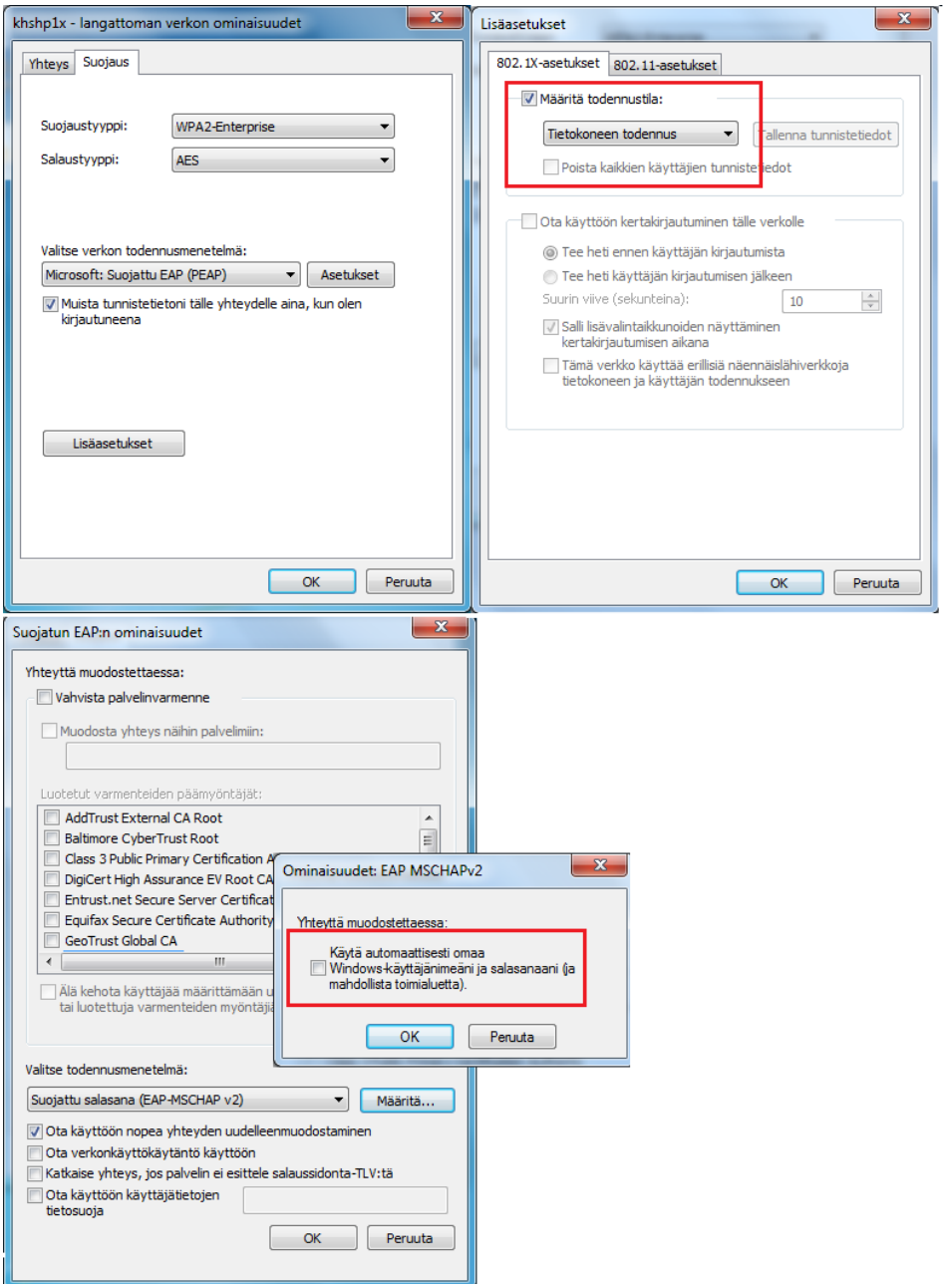


Kuva 57. Windows 7 802.1X natiivin LAN-supplikantin PEAP-konfiguraatio.

Liitteestä 5 voimme tarkastella kuinka laite autentikoituu ISE:llä onnistuneesti lankaverkkoon käyttäen autentikointi protokollana PEAP:a.

7.2.2 Windows 7 WLAN 802.1X EAP-PEAP Microsoftin supplikantilla

Myös langattomalla puolella riittää pelkkä natiivin supplikantin konfigurointi. Taas tulee muistaa 802.1X asetuksista määrittää todennustilaksi konetunnistus. Samoin EAP-MSCHAPv2-ominaisuuksista käyttäjätunnistus pois päältä yhteyttä muodostettaessa.



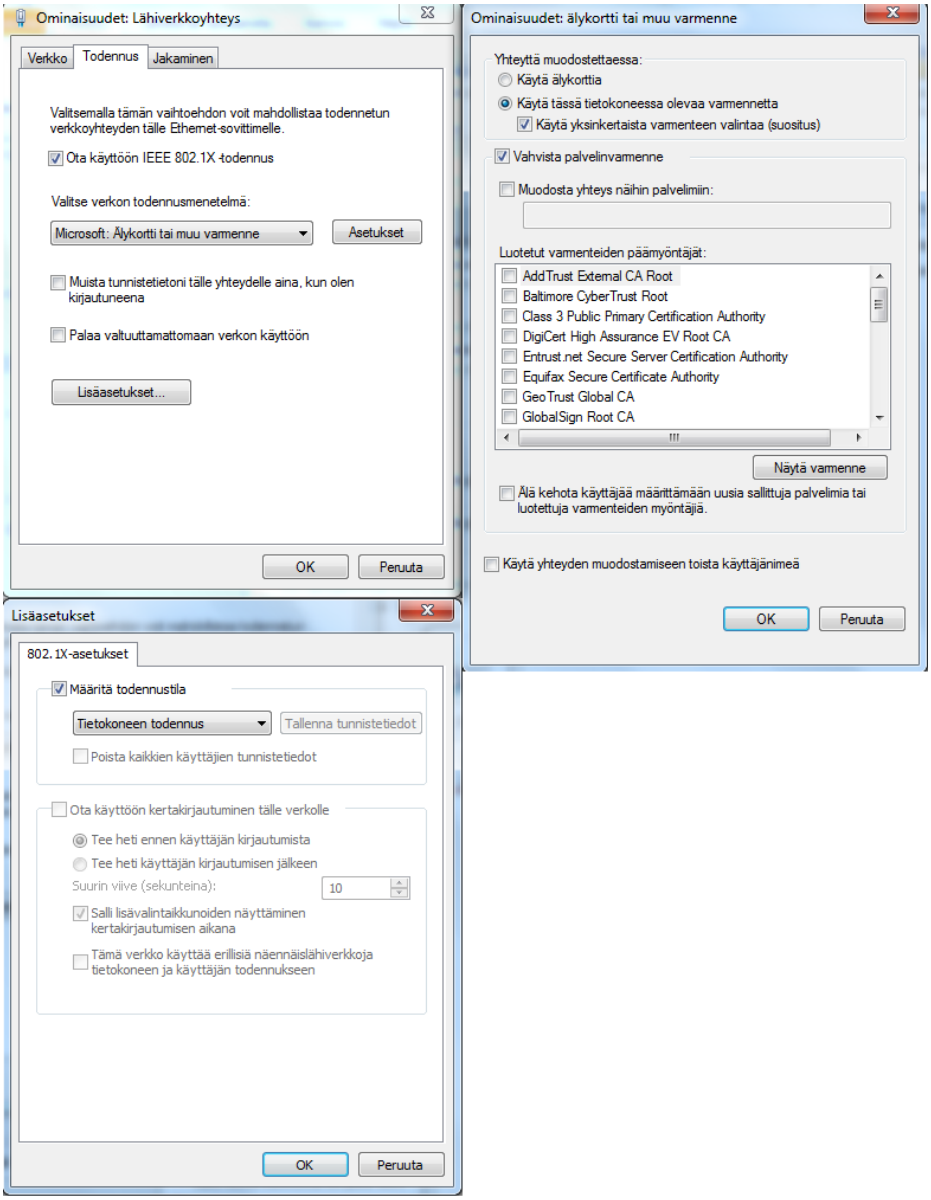
Kuva 58. Windows 7 802.1X natiivin WLAN-supplikantin PEAP-konfiguraatio.

ISE:ltä voimme havaita Windows 7 käyttöjärjestelmällä varustetun kannettavan tietokoneen onnistuneen 802.1X autentikaation käyttämällä EAP-PEAP:a.

7.2.3 Windows 7 LAN 802.1X EAP-TLS Microsoftin supplikantille

Jotta voidaan käyttää EAP-TLS autentikointi protokollaa, tulee työasemalla ja palvelimella olla sertifikaatit. Tätä tarkoitusta varten KHSHP:n verkkoon asennettiin oma sertifikaatti-infra. Kun työasema liitetään ”KHSHP C GPO CA Auto-enrollment”-ryhmään saa se uudelleen käynnistettäessä sertifikaatin. Konfiguroitaessa Windows 7:lle EAP-TLS valitaan todennusmenetelmäksi “Microsoft: Älykortti tai muu varmenne”. Varmenteen

ominaisuuksista valitaan ”Käytä tässä koneessa olevaa varmennetta” sekä ”Vahvista palvelinvarmenne”

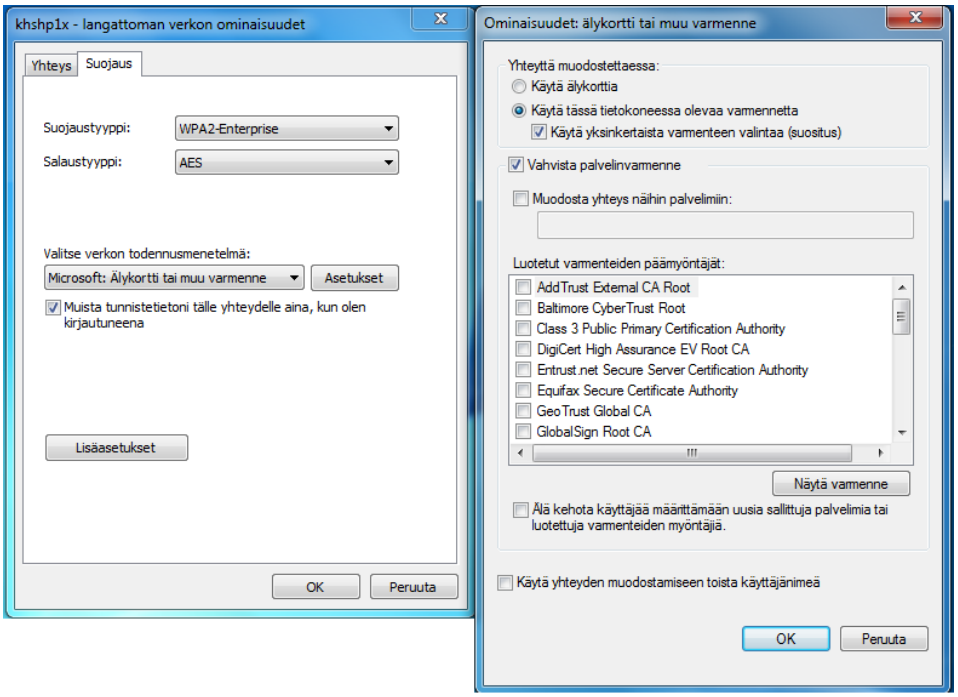


Kuva 59. Windows 7 EAP-TLS LAN-konfiguraatio natiiville supplikantille.

ISE:llä näkyy heti onnistunut autentikaatio. Laite on suorittanut koneautentikoinnin ja ohjattu PC-KHSHP profiiliin.

7.2.4 Windows 7 WLAN 802.1X EAP-TLS Microsoftin supplikantilla

EAP-TLS konfiguraatio langattomalle Windows 7 supplikantille on varsin yksinkertaista. Todennusmenetelmäksi valitaan sama kuin lankaverkossakin ”Microsoft: Älykortti tai muu varmenne” ja todennusmenetelmän ominaisuuksista ”Käytä tässä tietokoneessa olevaa varmennetta” sekä ”Vahvista palvelinvarmenne”.



Kuva 60. Windows 7 EAP-TLS WLAN-konfiguraatio natiiville supplikantille.

ISE:ltä voidaan tarkistaa, että autentikaatio on onnistunut.

7.3 Cisco Anyconnect konfigurointi

Anyconnect-supplikantin käyttämät verkkoprofiilit luodaan Anyconnect Profile Editorilla. Editorilla voidaan hallita client politiikat, autentikointi politiikat sekä erilaiset käytössä olevien verkkotyyppien ominaisuudet. Samoja Profile Editorilla luotuja configuraatio-profiileja voidaan käyttää sekä Windows XP:ssä että Windows 7:ssa. Eri käyttöjärjestelmillä vain polku, minne xml-muotoinen konfiguraatiotiedosto tallennetaan, vaihtelee.

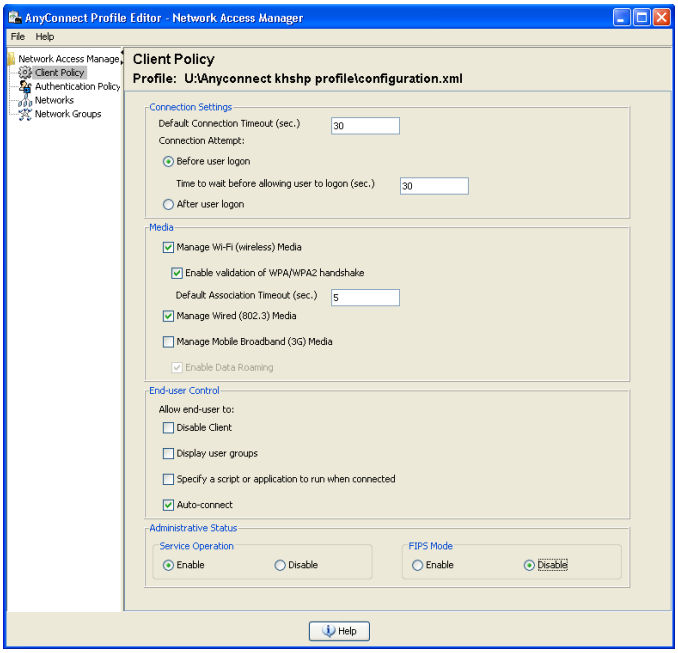
```
Win XP: c:\Documents And Settings\All Users\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml
```

```
Win 7: c:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml
```

Cisco Anyconnect Mobile Security Client-ohjelmistoon voidaan ladata erilaisia moduuleita. Sairaalalla Anyconnect sisältää Network Access Managerin eli NAM:n sekä VPN-moduulin. Seuraavassa käymme läpi konfiguraatiotiedoston luonnin, millä testaus eri käyttöjärjestelmillä ja autentikointimuodoilla suoritetaan.

7.3.1 Client Policy

Kuvasta 61 näemme kuinka perusasetukset kaikkien käyttöjärjestelmien clienteille voidaan konfiguroida. Yhteys pyritään muodostamaan aina ennen käyttäjän kirjautumista ja tälle annetaan 30 sekunnin aikaikkuna. Media-kohdasta valitaan mitä kaikkia yhteysmedioita Anyconnect hallinnoi. Sairaalalla ei toistaiseksi käytetä 3G.n yli mitään, joten 802.11 ja 802.3 – yhteydet riittävät. Loppukäyttäjän oikeuksia muokata supplikanttia voidaan myös konfiguroida. Nämä ovat asioita joita tulee käsitellä tarkemmin jos 802.1X:n sekä Anyconnectin käyttöönotosta tehdään sairaalalla myöntävä päätös.



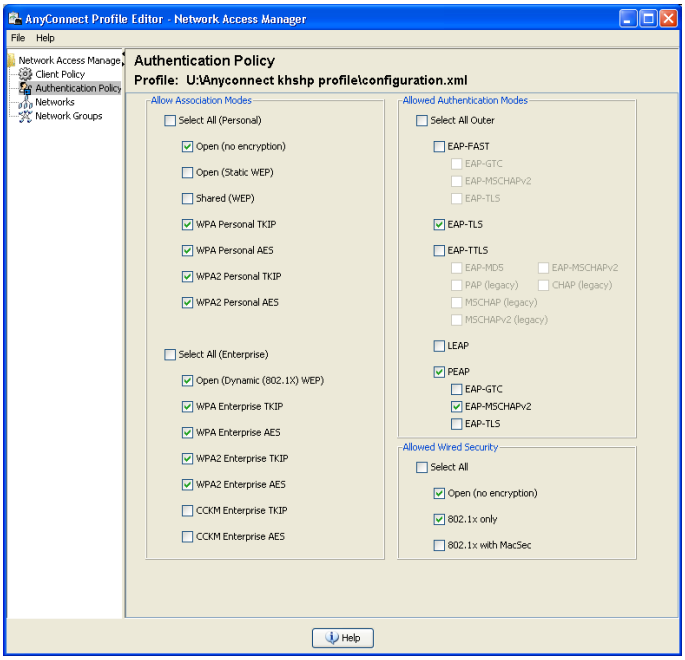
Kuva 61. Anyconnect Profile Editor Client Policy konfiguraatio.

”Service Operation”-ominaisuudella saadaan säädeltyä Anyconnectin kykyä hallita työasemien verkkoyhteyksiä. Jos Anyconnect halutaan nopeasti disabloida koko verkon alueelta, muokataan profiilia tästä kohtaa ja jaellaan uusi configuraatio GPO:na työasemille. Tällöin Windowsien oma supplikantti hoitaisi verkkoyhteydet. FIPS eli ”Federal Information Processing Standard” on Yhdysvaltojen valtion kehittelemä standardi, jolla säädellä kryptografisia vaatimuksia ja sitä ei oteta käyttöön.

7.3.2 Authentication Policy

”Authentication Policy”-kohdasta säädellään Anyconnect-clientissa sallittavia politiikkoja. Tämä tarkoittaa niitä assosiaatio ja autentikointi moodeja sekä lankaverkon tietoturvaa joita käyttäjä voi ottaa käyttöönsä. Jos Anyconnectin profiili lukitaan, eli estetään käyttäjältä mahdollisuus muokata omaa konfiguraatiotaan ei tässä kohdassa tarvita tarkkaa rajausta vaan itse network-profiilit suorittavat rajoitusten määrittelyn. Jos sen sijaan halutaan, että esimerkiksi lääkärit voivat käyttää konettaan kotiverkossa, jos-

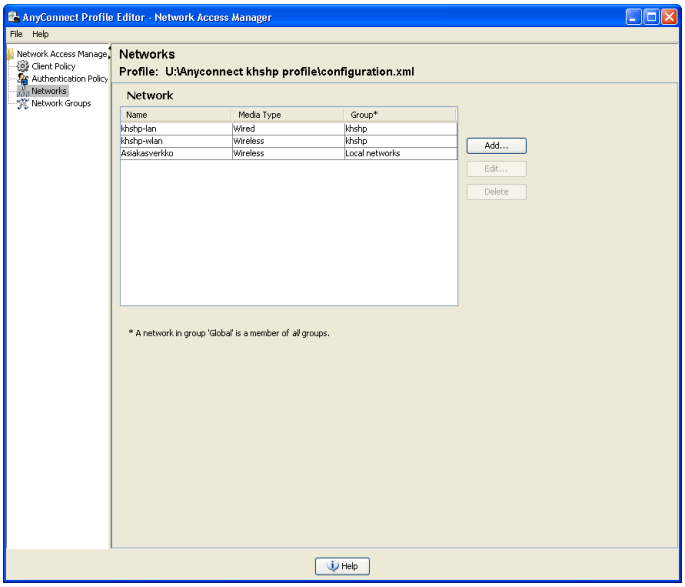
sa ei ole 802.1X päällä tulee käyttäjälle sallia tällaiset verkot. Sairaalan lopullinen tietoturvapolitiikka määrittelee, kuinka tullaan toimimaan.



Kuva 62. Anyconnect Profile Editorin sallimat autentikointi politiikat.

7.3.3 Networks

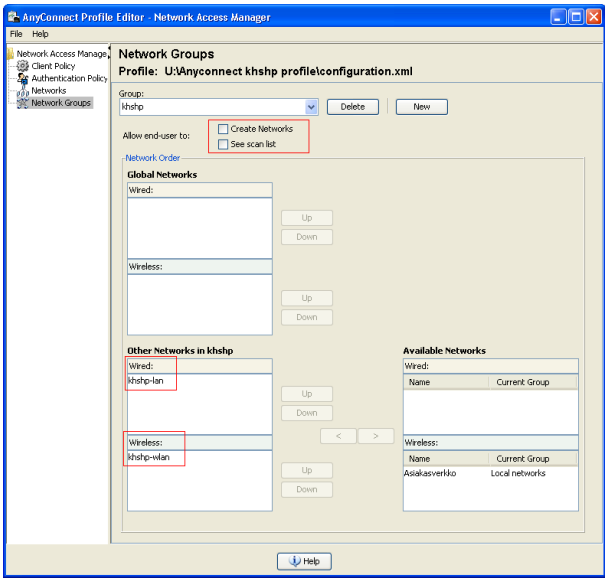
”Networks”-kohdassa voidaan luoda ennalta määriteltyjä verkkoja, joista käyttäjät voivat valita käyttöönsä haluamansa. Kuvasta 63 näemme esimerkin, miten verkot voivat olla määritelty. Kuvassa näkyy keskussairaalan oma suojattu lankaverkko sekä langaton verkko ja myös esimerkin vuoksi paikallisten verkkojen ryhmään sijoitettu langaton asiakasverkko. Eri ”Network”-profiilien alle voidaan määritellä tarkemmin ominaisuuksia eri verkoille, kuten tietoturva-asetuksia ja media tyyppejä. Verkkoprofiilit voidaan sitoa erillisiin verkkoryhmiin eli Network Groupseihin.



Kuva 63. Anyconnect Profile Editor Networks.

7.3.4 Network Groups

Network groupit antavat mahdollisuuden hallita loppukäyttäjien mahdollisuuksia luoda tai liittyä muihin kuin pääkäyttäjän määrittelemiin verkkoihin. Kuvasta 64 näemme, että ryhmässä ”khshp” loppukäyttäjät eivät näe muita, kuin ryhmään määritellyt ”khshp-lan” ja ”khshp-wlan”-verkot. Loppukäyttäjä ei voi myöskään lisätä tähän ryhmään muita verkkoja. Halutessaan pääkäyttäjä voi lukita tämän profiilin sairaalan hallinnassa oleviin laitteisiin. Tällöin näillä laitteilla ei voisi ottaa yhteyttä mihinkään muihin, kuin KHSHP:n hallinnoimiin verkkoihin. Paljon lisää tietoturvaa, mutta rajoittaa mobiililaitteiden käytön pelkästään sairaalan alueelle. Esimerkiksi vierailtaessa muissa sairaaloissa tai yrityksissä ei verkkoyhteyttä olisi mahdollista saada. Tämäkin asia pitää käydä tarkemmin läpi jos Anyconnect otetaan sairaalalla laajemmin käyttöön.

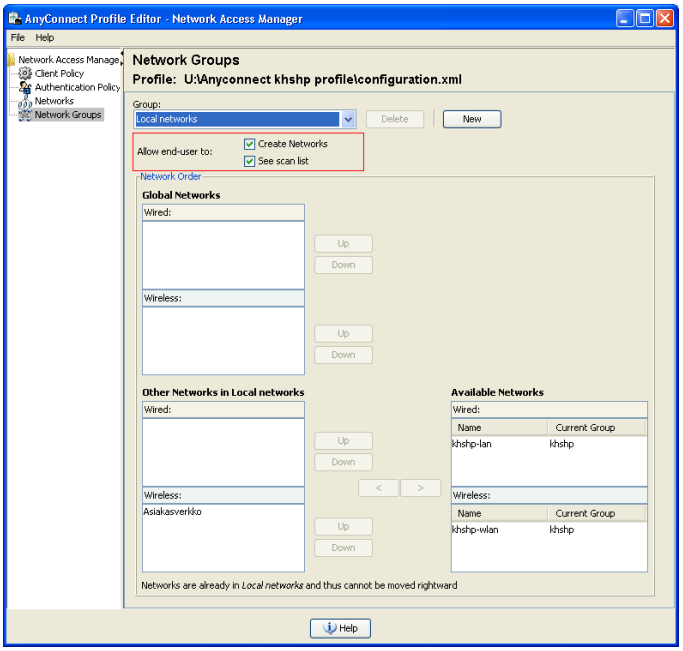


Kuva 64. Anyconnect Profile Editor Network Groups.

”Local networks”-ryhmään käyttäjälle voidaan halutessa sallia kolmansien osapuolien verkkojen näkyvyys, sekä mahdollisuus lisätä omia verkkoja, esimerkiksi oma langaton kotiverkko. Tämä mahdollisuus voidaan helposti jättää pois, jos sairaalan hallinnoimien laitteiden ei haluta päästä muihin kuin sairaalan hallinnassa oleviin verkkoihin. Kuvassa 65 on ”Local Networks”-ryhmässä sallittu kolmansien osapuolien verkkojen näkyvyys sekä loppukäyttäjän mahdollisuus lisätä omia verkkojaan. Ryhmään on esimerkin vuoksi luotu ”Asiakasverkko”-profiili, vaikka tuo SSID onkin avoin ja tulisi näkyviin joka tapauksessa (jos ”see scan list” sallittu).

Jos halutaan luoda vaikkapa lääkereille ryhmä kannettavia tietokoneita, joissa sallitaan muiden verkkojen käyttö, onnistuu tämä helposti luomalla tähän oma profiili. Nuo kannettavat tietokoneet sitten lisättäisiin tiettyyn omaan ryhmäkäytäntöönsä, jolla sitten tuo uusi Anyconnect-profiili jael-

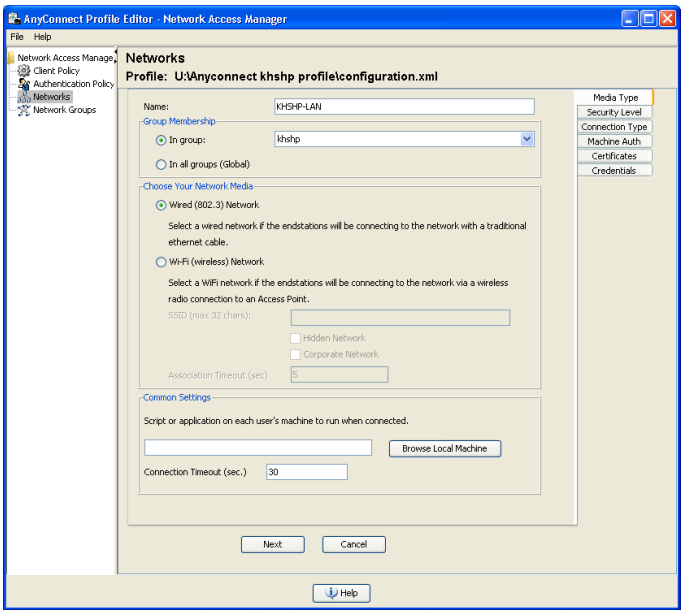
taisiin. Näin voitaisiin sallia joustavampi mutta hallittavissa oleva verkkokäyttö tietyille laitteille.



Kuva 65. Anyconnect Network Groups – Local Networks

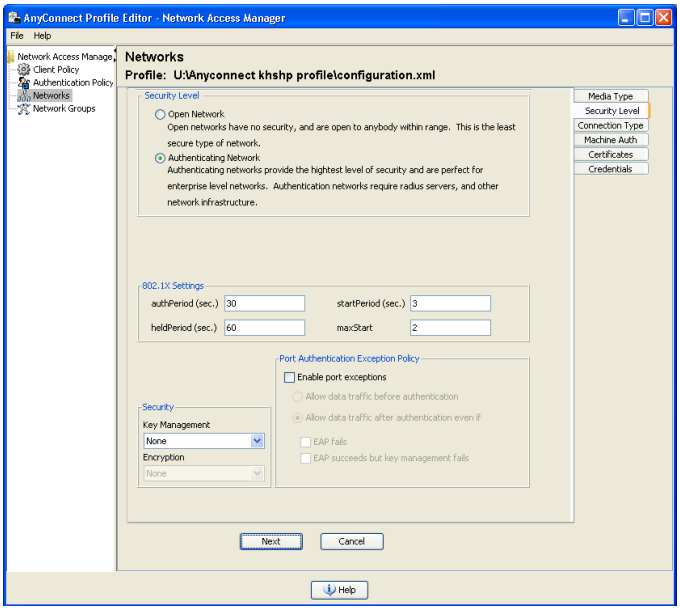
7.3.5 Network Profile KHSHP-LAN

Sairaalan langallista lähiverkkoa varten luodaan profiili ”KHSHP-LAN”. Ensimmäiseksi määritellään asetukset ”Media Type”-välilehdeltä. Profiili liitetään ryhmään khshp, jonka alle kaikki sairaalan hallinnassa olevat verkot sijoitetaan. Käytettäväksi mediaksi valitaan langallinen verkko. Toistaiseksi koneille ei ajeta Anyconnectin kautta mitään skriptejä tai muita ohjelmia. yhteyden aikarajaksi määritetään 30 sekuntia, jonka jälkeen anyconnect ilmoittaa ”No network connectivity” (kuva 27).



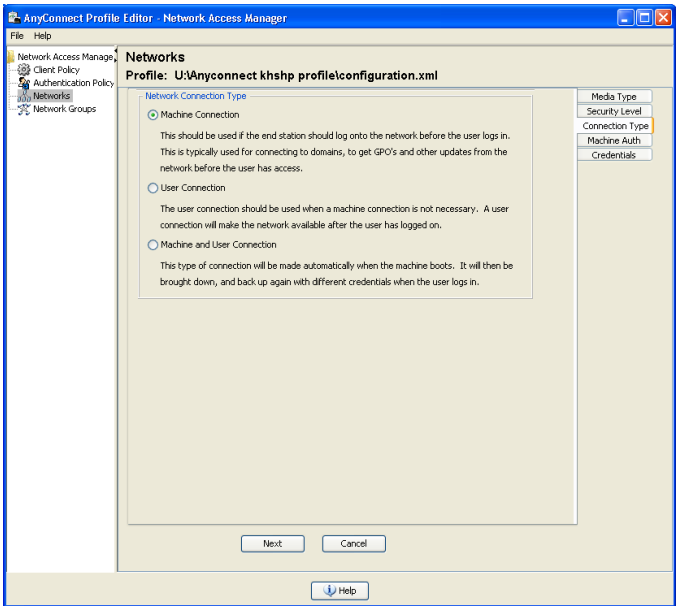
Kuva 66. Anyconnect Profile Editor KHSHP-LAN Media type

Seuraava välilehti on nimeltään ”Security Level”. Täältä määritellään verkoksi autentikoiva verkko sekä aikarajat 802.1X yhteyksille. Verkko voidaan myös jättää täysin avoimeksi (kuva 67).



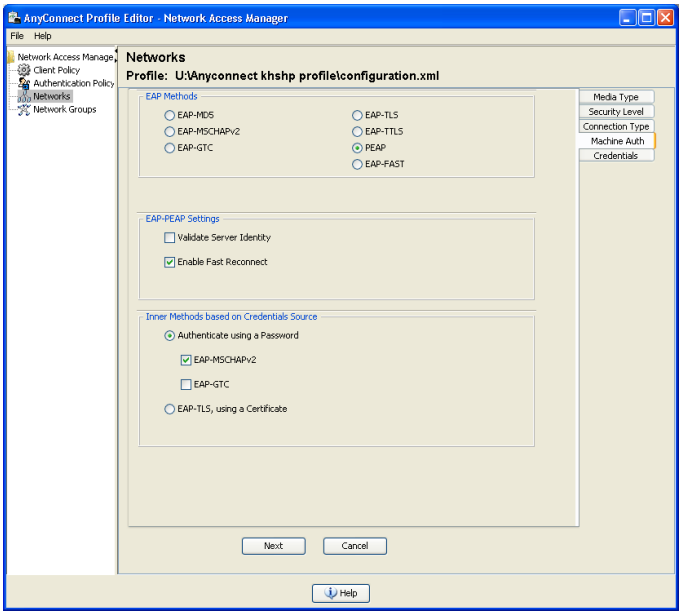
Kuva 67. Anyconnect Profile Editor KHSHP-LAN Security Level

“Connection Type”-välilehdeltä voidaan määritellä miten käyttäjä tai kone autentikoidaan yhteyden muodostukseen nähden. Sairaalan tapauksessa valitsemme ”Machine Authentication”, jotta tarvittavat GPO:t saadaan ladattua koneelle ennen käyttäjän kirjautumista (kuva 68).



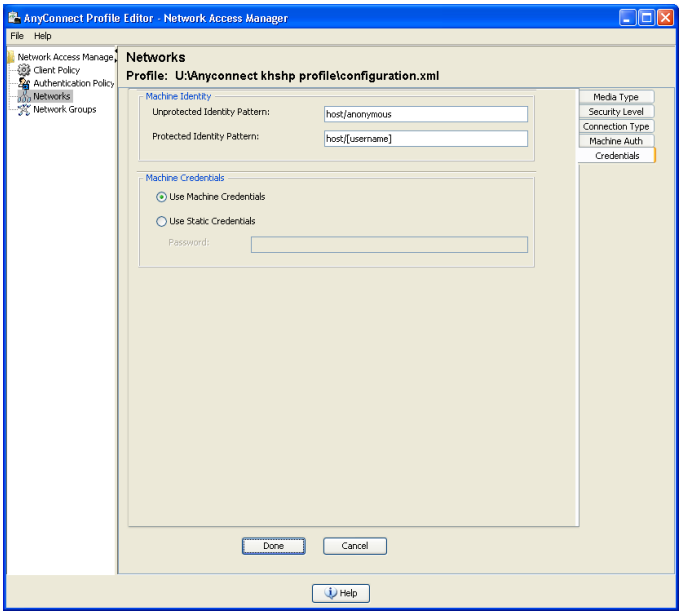
Kuva 68. Anyconnect Profile Editor KHSHP-LAN Connection Type.

Koska “Connection Type”-kohdassa valittiin koneautentikointi, on seuraavana välilehtenä “Machine Auth”. Jos tyypiksi olisi valittu käyttäjäautentikointi, olisi tässä nyt ”User Auth” ja molemmat jos käytettäisiin yhdessä sekä käyttäjä- että koneautentikointia. Kuvassa 69 näkyy asetukset, jotka valitaan käytettäessä EAP-PEAP-metodia. Nämä asetukset vaihtelevat käytetyn EAP-Methodin mukaan.



Kuva 69. Anyconnect Profile Editor KHSHP-LAN Machine Auth.

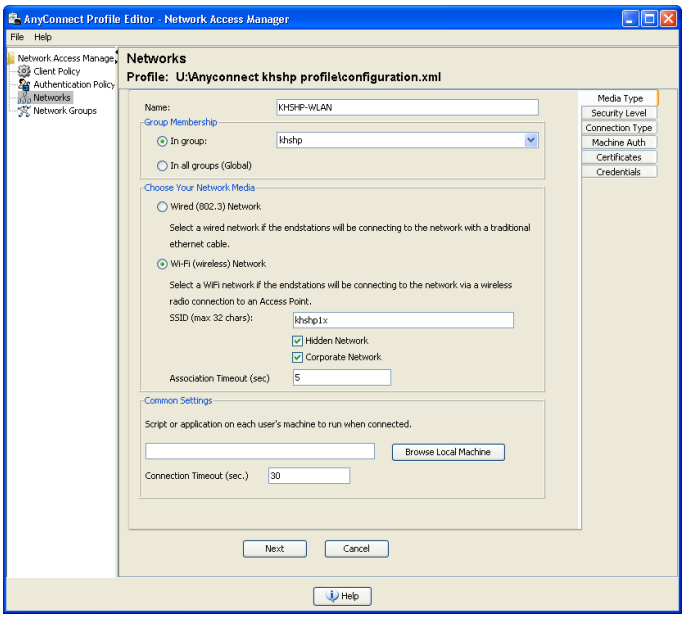
Viimeiseksi ”Credentials”-välilehdeltä määritellään, missä muodossa autentikoivan koneen suojattu identiteetti annetaan. KHSHP:n tapauksessa kone esitellään muodossa ”host/[username]”. Kun käytössä ei ole konesertifikaattia (EAP-PEAP) [username] tarkoittaa koneen nimeä, ei itse käyttäjän tunnusta (kuva 70).



Kuva 70. Anyconnect Profile Editor KHSHP-LAN Credentials.

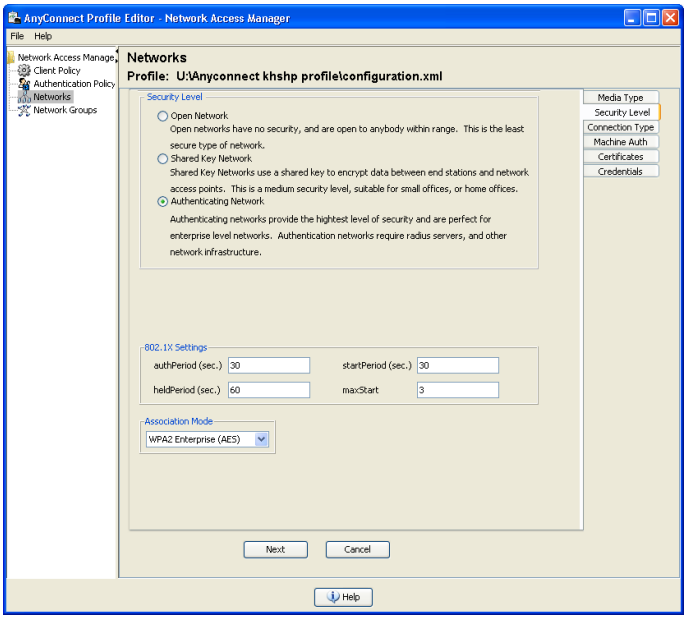
7.3.6 Network Profile KHSHP-WLAN

Sairaalan langatonta verkkoa varten luodaan profiili ”KHSHP-WLAN”. Profiilin ”Media Type”-välilehdeltä määritellään ryhmäksi ”khshp”. Käytettäväksi mediaksi valitaan langatonta verkkoa vastaava ”Wi-Fi”. Tämän alle määritellään käytettävä SSID, sekä kerrotaan tämän olevan piiloitettu verkko. ”Corporate Network” tarkoittaa, että kyseessä on sairaalan oma verkko. Tähän langattomaan verkkoon yhdistetään aina ensimmäisenä, vaikka SSID:tä ei broadcastattaisi, ja vaikka alueella olisi muitakin mahdollisia langattomia verkkoja.



Kuva 71. Anyconnect Profile Editor KHSHP-WLAN Media Type.

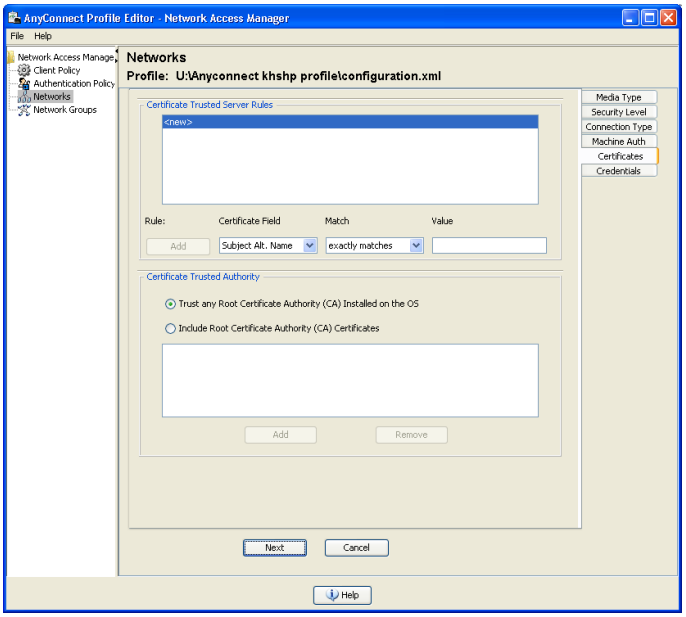
“Security Level”-välilehdellä ei ole muuta eroa lankaverkkoon, kuin liityntämuodon valinta. Sairaalan tapauksessa tämä on ”WPA2 Enterprise (AES)”.



Kuva 72. Anyconnect Profile Editor KHSHP-WLAN Security Level.

“Connection Type”, ”Machine Type” ja ”Credentials” ovat täysin samat langallisen verkon määrittelyn kanssa.

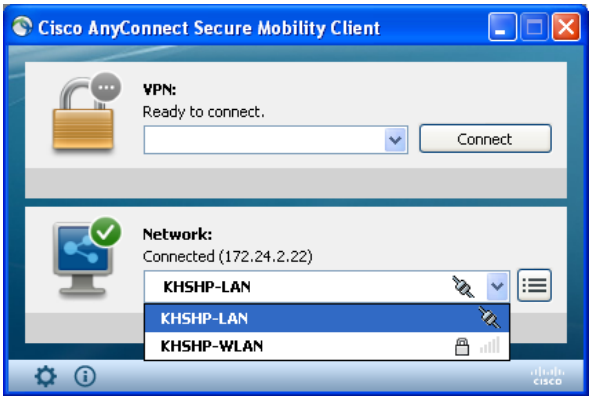
”Certificates”-välilehdelle ei tarvitse tehdä muutoksia EAP-PEAP:n ollessa käytössä. Tähän voitaisiin määritellä erilaisia sääntöjä koskien sertifikaatteja.



Kuva 73. Anyconnect Profile Editor KHSHP-WLAN Certificates.

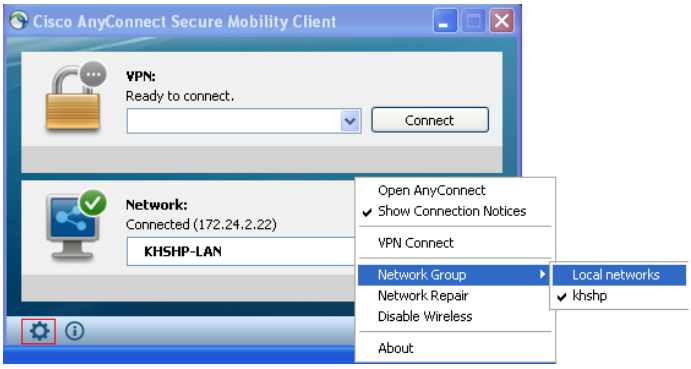
7.4 Cisco Anyconnect testaus

Kuten muidenkin supplikanttien osalta, keretään Anyconnectillakin lähinnä testaamaan ohjelman ja tunnistautumismenetelmien toimivuutta ja yhteensopivuutta eri käyttöjärjestelmillä. Ennen päätöstä todellisesta käyttöönotosta tuotantoverkossa, tulee suorittaa pidempiaikainen ja laajempi testaus.



Kuva 74. Anyconnectin supplikantti. Ylempänä VPN-moduuli, alempana NAM.

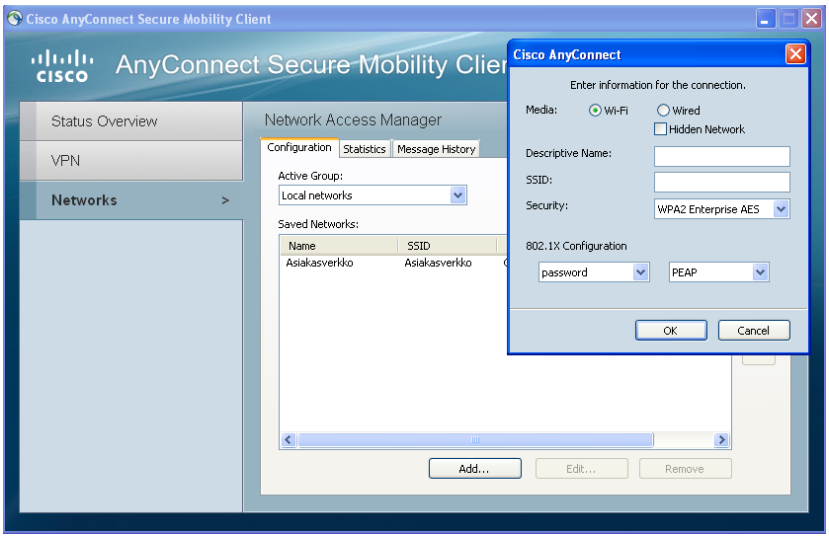
Kuvasta 74 näemme kuinka käyttäjä voi valita ”Network Access Managerista” eli NAM-moduulista vain sairaalan hallinnoimat verkot. Jotta käyttäjä voisi valita kolmansien osapuolien lokaaleja verkkoja, tulee ”Network Group”-kohdasta valita ”Local networks”. Ryhmän voi vaihtaa painamalla Anyconnectin kuvaketta oikealla hiirennapilla ja valitsemalla ”Network Group – Local networks” (kuva 75). Jos käyttäjä valitsee sairaalan alueella ”Local networks”-ryhmän yhdistyy NAM konfiguraatiossa määriteltyyn ”Asiakasverkko”-SSID:een. Tämän ryhmän alle tulevat myös käyttäjän omat verkot jos näin halutaan sallia.



Kuva 75. Anyconnect NAM Network Groupin vaihto.

Oma verkko voidaan luoda painamalla kuvassa 38 punaisella korostettua nappia. Näin aukeaa ”Advanced”-valikko, josta voi seurata sen hetkisen verkon ja VPN-yhteyden tietoja sekä konfiguroida omia verkkoja. Jos verkkoryhmänä on ”khshp” on ”add”-painike harmaana, eikä käyttäjä voi lisätä tänne mitään. Valitessa aktiiviseksi ryhmäksi ”Local networks” käyttäjä pystyy konfiguroimaan omia verkkoja. Kuvassa 76 on esitetty konfigurointi-ikkuna, johon käyttäjä saa määrittää oman tai jonkun muun kolmannen osapuolen verkon asetukset.

Jokaisen muutoksen jälkeen ei ole välttämätöntä käynnistää konetta uudestaan. Anyconnectissa on ”Network repair”-ominaisuus, jota painamalla se käynnistää verkkolaitteet uudestaan ja näin ollen resetoi kaikki interfacet. Tämä vastaa verkkolaitteiden osalta koneen uudelleenkäynnistämistä. GPO:n latautumisen testaamiseksi on kuitenkin hyvä suorittaa koneen uudelleenkäynnistys.



Kuva 76. Anyconnect NAM Advanced Options – uuden verkon lisääminen.

7.4.1 Win XP LAN 802.1X EAP-PEAP Ciscon Anyconnectilla

Yhteys muodostuu hyvissä ajoin ennen Windowsiin kirjautumista. NAM-profiili haistelee itsestään käytössä olevan LAN-yhteyden ja lataa tämän mukaan KHSHP-LAN-verkkoprofiilin. ISE:llä näkyy onnistunut PEAP-tunnelointi sekä autentikointi EAP-MSCHAPv2:lla. Konfiguraatio autentikoinnille on kuvan 69 mukainen.

7.4.2 Win XP LAN 802.1X EAP-TLS Ciscon Anyconnectilla

Jotta EAP-TLS saataisiin käyttöön tulee Profile Editorilla tehdä pieni muutos KHSHP-LAN-verkon ”Machine Auth”-kohtaan. Kuvassa 69 näkyvän PEAP:n tilalle vaihdetaan EAP-TLS. Käynnistettäessä kone uudelleen, nousee verkkoyhteys ylös ennen sisäänkirjautumisikkunaa. ISE:lle tulee näkyviin onnistunut EAP-TLS-autentikaatio.

7.4.3 Win XP WLAN 802.1X EAP-PEAP Ciscon Anyconnectilla

Koneen käynnistyessä voidaan langatonta autentikaatiota tarkkailla suoraan ISE:ltä. Huomataan, että kannettava tietokone autentikoituu WLC:n kautta samalla kun Windowssin käynnistysikkunassa lukee ”Valmistellaan verkkoyhteyksiä” eli onnistuneesti ennen kirjautumista. PEAP-konfiguraatio on langattomalla supplikantilla kuvan 69 mukainen.

7.4.4 Win XP WLAN 802.1X EAP-TLS Ciscon Anyconnectilla

Langattomassa supplikantissa muutoksen tekeminen EAP-PEAP:sta EAP-TLS:yyn on yhtä nopeaa kuin lankaverkossakin. Ainut muutos on koneautentikoinnin alta EAP-TLS:n valinta. Koneen käynnistyessä langaton yhteys nousee jopa hieman nopeammin ylös verrattuna EAP-PEAP:aan. ISE:ltä voidaan todeta onnistunut EAP-TLS koneautentikointi.

7.4.5 Windows 7 LAN 802.1X EAP-PEAP Ciscon Anyconnectilla

Windows 7-käyttöjärjestelmällä testataan täysin samaa konfiguraatiotiedostoa, jota käytettiin Windows XP:ssä. Vain tiedoston asennuspolku muuttuu. Uudelleenkäynnistyksen myötä todetaan EAP-PEAP-autentikoinnin toimivan moitteetta ennen sisäänkirjautumista. Tämä todistaa sen, että jaeltaessa konfiguraatioita sairaalan tuotantoverkon koneille, ei tarvitse välittää konfiguraatiomuutoksista eri käyttöjärjestelmille, kunhan polku määritellään oikein.

7.4.6 Windows 7 LAN 802.1X EAP-TLS Ciscon Anyconnectilla

EAP-TLS yhteyteen tarvitaan sama muutos konfiguraatioon, kuin XP:n puolella. Uudelleenkäynnistyksen jälkeen autentikointi tapahtuu ennen sisäänkirajutumista ilman ongelmia.

7.4.7 Windows 7 WLAN 802.1X EAP-PEAP Ciscon Anyconnectilla

Konfiguraatio Windows XP:n kanssa täysin identtinen. Toimii moitteetta, yhteys muodostuu Windows 7:lla langattomassa verkossa huomattavasti nopeammin käynnistyksen yhteydessä verrattuna XP:een.

7.4.8 Windows 7 WLAN 802.1X EAP-TLS Ciscon Anyconnectilla

EAP-TLS:n kohdalla ei konfiguraatioon myöskään muutoksia. Ainut ero XP-koneisiin on nopeampi yhteyden muodostus. Ei havaittavia ongelimia.

7.5 Mac Authentication Bypass testaus

Laitteet jotka eivät tue 802.1X autentikointia pitää kuitenkin saada sairaalalla autentikoivien porttien läpi verkkoon. Tällaisia laitteita ovat pääasiassa verkkotulostimet ja lääkintälaitteet. ISE:lle pitää luoda tietokanta, johon haluttujen laitteiden MAC-osoitteet kerätään.

Testauksessa käytetään vanhahkoa Hewlet Packardin P3005n JetDirect-tulostinta. Tulostin ei kykene 802.1X autentikointiin vaan sille tulee konfiguroida MAB. ISE:ssä mennään ”Administration – Identity Management – Endpoints”-valikkoon. Tänne lisätään uusi Endpoint eli päätelaite. Laitteesta tarvitaan MAC-osoite sekä valitaan käytettävä Endpoint policy.

Kuva 77. Tulostimen lisääminen Endpoints –listaan MAB:n mahdollistamiseksi.

Liitteestä 6 näemme kuinka verkkotulostimen autentikointi on ensiksi punaisella, eli epäonnistunut, mutta Endpoints-listaan lisäämisen jälkeen MAB-autentikointipolitiikka on löytynyt ja tulostin on autorisoitu sairaalan verkkoon.

8 RAPORTOINTI JA VIANSELVITYS

Verkkolaitteiden näkyvyyden parantuessa raportointi ja vikojen selvitys helpottuu. ISE:n ja Primen tuottama data auttaa pääkäyttäjiä tuottamaan parempia ja luotettavampia palveluita sekä vastaamaan verkon haasteisiin ja käyttäjien ongelmatilanteisiin reaaliaikaisemmin.

8.1 ISE Raportointi ja vianselvitys

ISE tuottaa kokoajan tietoa koko verkon alueelta ja tiivistää sen raporteiksi joita pääkäyttäjät voivat käyttää hyväkseen. Raportteja saa ISE:stä yksittäisten laitteiden tai käyttäjien autentikoinnista aina koko verkon laajuisiin ”Posture checkeihin” asti. Esimerkkinä voimme käyttää testikytkimeltä saatua dataa. Raportti on yleiskatsaus kyseisen kytkimen eli autentikaattorin suorittamista autentikoinneista (liite 7). Raportista ilmenee autentikointien keskimääräinen kesto sekä maksimi vasteajat. Jos käyttäjät ilmoittavat jollain alueella verkkoon liitynnän hitaudesta, voidaan ISE:ltä ottaa raportti tuon alueen autentikaattoreista ja tutkia onko kyse kytkimistä vai vaikkapa supplikanteista.

ISE:n ”Live Authentications”-näkymä toimii myös reaaliaikaisena raportointityökaluna. Se säilyttää tosin vain viimeiset 24 tunnin tiedot, mutta selkeä graafinen näkymä auttaa pääkäyttäjiä huomaamaan heti autentikoinnit jotka eivät syystä tai toisesta mene halutusta tietoturvapolitiikasta läpi. Liitteissä 1-6 on näkyvissä leikkeleitä tästä näkymästä ja työn aikana tämä oli ylivoimaisesti tärkein, helppokäyttöisin ja paras tapa testata kuinka laitteet reagoivat eri konfiguraatioihin.

ISE:en voidaan luoda myös mitä moninaisimpia muokattuja hälytyksiä, jotka kertovat jos verkossa tapahtuu jotakin tiettyä joko virheellistä tai rikollista toimintaa. Tätä ominaisuutta ei keretty työn aikana testaamaan.

Toinen ajanpuutteen vuoksi pois jäänyt toiminto on erinomainen ”Posture Policy”. Tällä tominnolla voidaan luodata päätelaitteiden virusturvan ja käyttöjärjestelmäpäivitysten ajantasaisuutta ja tähän vedoten esimerkiksi estää pääsy vanhentuneet virustunnisteet omaavilta koneilta tyystin. Posturesta saatava raportointi antaa tietoa verkkoon päästettyjen ja pyrkineiden laitteiden tilasta laaja-alaisesti.

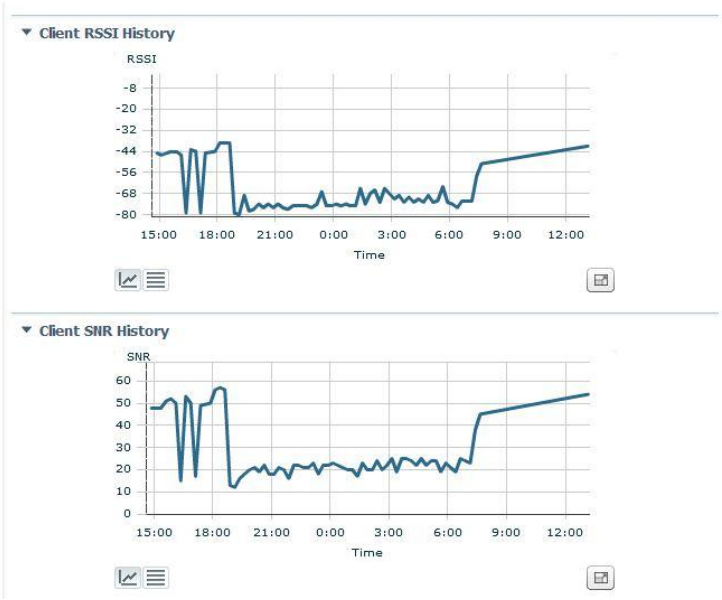
8.2 Prime raportointi ja vianselvitys

Valitettavasti myös Primen testaamista ei saatu suoritettua halutulla laajuudella. Testin aikana kuitenkin tuli selväksi, kuinka tärkeä työkalu Prime olisi sairaalan verkon hallinnassa. Varsinkin langattoman verkon ongelmat saatasisiin käsiteltyä paremmin, sillä prime kerää langattomista päätelaitteista dataa reaaliaikaisesti ja tuottaa tästä historiatietoa. Näin ollen tukipyynnön tullessa, voitaisiin kyseisen käyttäjän ja työaseman liikkeitä ja

toimintaa verkossa tarkastella takautuvasti. Kun nähtäisiin esimerkiksi työaseman hyppiminen villisti kahden tukiaseman välillä, kuten kuvassa 78, voitaisiin helposti päätellä pätkinnän johtuvan tästä.

Kuva 78. Prime – Työaseman assosioinnit tukiaseman kanssa.

Primella saadaan myös tarkkaa tietoa työaseman langattoman verkon signaalitasoista, joita voidaan sitten verrata vikailmoitusten ajankohtiin. Näin saadaan vankkaa tukea vikaselvitykseen ja päätelmiin ongelmien syistä.



Kuva 79. Prime – Historiatietoa työaseman käyttämästä WLAN-signaalista.

Primellä voidaan myös hakea käyttäjiä tai koneita erikseen. Kun käytössä on 802.1X-autentikointi, saadaan suoraa tieto missä autentikaattorissa käyttäjä tai laite on kiinni. Hakuja voidaan suorittaa käyttäjä- tai konenimen perusteella, IP- tai MAC-osoitteilla tai suoraa kysyä ”kuka tai mikä tässä portissa toimii?”. Prime antaa kyselyistä listauksen ja näistä valitsemalla haluttu saadaan tarkempaa tietoa kyseisestä kohteesta. Enää ei tarvitsisi etsiä työasemia hitaasti CLI:lla MAC-osotteiden perusteella. Koneen nimi hakukenttään riittää.

Kuva 80. ”PCH2012” –konehaun tulokset Primellä.

Primestä saa ulos myös lukuisia analyysejä ja raportteja eri valmistajien laitteiden osuuksista verkossa, kokonaiskaistankäytöstä, kaistankäytöstä ohjelmakohtaisesti, missä verkossa on minkäkin verran käyttäjiä ja niin edelleen. Kaikki tämä on todella hyödyllistä tietoa suunniteltaessa verkon kehitystä käyttäjien tarpeita vastaavaksi.

9 JOHTOPÄÄTÖKSET

Kevään 2013 aikana toteutettu muutaman kuukauden testijakso poiki positiivisia tuloksia ja kokemuksia identiteettitietoisesta verkkoarkkitehtuurista ja sen mahdollisuuksista Kanta-Hämeen Keskussairaalalla. 802.1X autentikointiin perustuva pääsynhallinta arkkitehtuuri Cisco Systemsin laitteilla todettiin varsin toimivaksi ja helposti käyttöön otettavaksi ratkaisuksi. Testauksen voidaan todeta olleen kaikin puolin onnistunut. Sen aikana tietotaito aiheesta kasvoi huomattavasti ja kaikki asetetut tavoitteet saatiin saavutettua.

Molempien käyttöjärjestelmien, sekä käytössä olevan Windows XP:n, että tulevan Windows 7:n supplikantit saatiin testattua kaikilla halutuilla autentikaatiomuodoilla. Myös Ciscon Anyconnect testattiin perinpohjaisesti. Todettakoon, että kaikki autentikointimenetelmät saatiin kaikilla supplikanteilla toimimaan, mutta eroja kuitenkin löytyi. Käyttöjärjestelmissä on selkeitä perusteellisia nopeuseroja jo sinälläänkin, joten ei ollut yllätys, että Windows 7:lla suoritetut testit tuottivat parhaan tuloksen. Windows 7:n omassa supplikantissa ja Ciscon Anyconnectissa ei oikeastaan ollut nopeudellisia eroja. Erot syntyvätkin konfiguroinnin helppoudessa ja selkeydessä, sekä yksinkertaisen ryhmäkäytännöillä suoritettavan profiilijakelun myötä. Ciscon Anyconnect oli ylivoimaisesti varmin toiminnassaan. Windows XP:tä ei ole alunperinkään luotu tukemaan 802.1X:ää, joten on sanomattakin selvää, että tämä kolmannen osapuolen supplikantti saavutti huomattavat erot verrattuna XP:n omaan supplikanttiin. Anyconnectilla yhteys saatiin varmasti toimimaan ennen kirjautumista kaikissa testiskenaarioissa ja tämä oli yksi tärkeimmistä kriteereistä, jotta tarvittavat ryhmäkäytännöt saadaan koneille.

Myös alussa huolestuttanut lääkintälaitteiden ja muun 802.1X:ää tukemattoman laitekannan saattaminen suojatun verkon kanssa yhteistoimintaan osoittautui turhaksi. ISE:stä löytyvät ominaisuudet, kuten MAB, mahdollistivat tiukan autentikoinnin ohittamisen, silti parantamalla tietoturvaa nykyisestä. Eri lääkintälaitejärjestelmien kanssa tulee silti vielä suorittaa lisätestausta ennen todellista käyttöönottoa sillä lääkintätekniikassa jokainen järjestelmä on uniikki. MAC-osotteiden avulla suoritetut ohitukset vaikuttivat kuitenkin varsin tehokkaalta tavalta.

Testattavaakin jäi vielä melkoisesti. Prime-järjestelmää ei keretty lisenssiongelmien myötä testaamaan tarpeeksi. Se vähä mitä siitä käteen jäi oli kuitenkin pelkästään positiivista. Primen avulla suoritetut käyttäjä- ja konehaut olivat niin käteviä ja nopeita, että jo ne yksinänsä tehostaisivat toimintaa sairaalalla huomattavasti. Puhumattakaan keskitetystä konfiguraatioiden ja softapäivitysten jakelusta kytkimille, sekä laajoista raportointimahdollisuuksista. ISE:n osalta testaamatta jäi todella tärkeä profilointi. Profiloinnin avulla verkosta voidaan etsiä haluttuja laitteita tai laitekantoja. Tämä kuitenkin estyi, sillä Fujitsun Konalan konesalissa testauksen ajan virtualisoituna sijainnut Identity Services Engine ei päässyt skannaamaan verkkoamme halutusti. Virtuaalikoneelta olisi pitänyt päästä muuttamaan virtuaalikytkimen ominaisuuksita ”Promiscous Mode” päälle. Tätä

ei kuitenkaan testin puitteissa saatu muutettua. Myös ISE:n ”Posture”-ominaisuus jäi täysin testaamatta. Tuo olisi vaatinut Advanced-lisenssin ISE:en, joten testauskokoonpanossa se oli mahdotonta. Posture toisi suuresti lisää tietoturvaa ihmisten omiin tai muissa verkoissa käytettyjen sairaalan laitteiden liittyessä sairaalan verkkoon. Laitteille suoritettaisiin aina niin kutsuttu ”Posture Check” jolla varmistettaisiin virusturvan ja käyttöjärjestelmäpäivitysten ajantasaisuus. Todella tärkeä asia pohdittavaksi tulevaisuuden hankintoja ajatellen. WEB-autentikointi jäi testauksen ulkopuolelle, sillä testauksen aikana huomattiin osan sairaalan WLAN-tukiasemista olevan liian vanhoja tukemaan WLC:n uudempaa versiota, jolle tuo WEB-pohja olisi rakennettu.

Jos verrataan uutta ISE:n päälle rakennettua pääsynhallintakokonaisuutta nykyiseen käytössä olevaan ratkaisuun ovat erot valtavia. Tulokset osoittivat, että uusi järjestelmä on ensinnäkin sairaalan resursseilla mahdollista toteuttaa. Toisekseen tietoturvan kasvaminen jättiaskelin ei voi koskaan olla huono asia. Varsinkaan kun se pystyttäisiin toteuttamaan käyttäjäystävällisesti ilman, että kenenkään käyttökokemus transitiovaiheessa kärsisi. Käyttäjät eivät periaattessa edes huomaisi eroa uuden ja vanhan välillä. Enintään supplikantin muutos Anyconnectiin voisi hämmentää aluksi, mutta käyttäjien ei kuitenkaan siitäkään tarvitsisi välittää. Suosittelenkin Sairaanhoitopiirille Anyconnectin ottamista käyttöön mahdollisimman pian. Vähintään ainakin kannettaviin tietokoneisiin. Pelkkä integroitu ja jo olemassa olevalla infralla toimiva VPN-palvelukin riittää tähän perusteluksi puhumattakaan sen ylivoimaisista ominaisuuksita 802.1X-puolella.
Suosittelisin myös ISE:n hankkimista. Sen tarjoamat tietoturvaominaisuudet nykyiseen nähden ovat niin valtavia, että Sairaanhoitopiirin on täysin perusteltua panostaa tähän asiaan taloudellisesti.

LÄHTEET

Kanta-Hämeen Sairaanhoitopiirin Suoriteraportti 3b 2012

IEEE Std 802.1X-2010
(http://standards.ieee.org/getieee802/download/802b-2004.pdf)

Implementing 802.1X Security Solutions for Wired and Wireless Networks Jim Geier, James T. Geier

Cisco 2011, BRKSEC-2005 - Deploying Wired 802.1x
(http://d2zmdbbm9feqrf.cloudfront.net/2011/anz/pdf/BRKSEC-2005.pdf)

https://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_2.0/trustsec_2.0_dig.pdf

http://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_overview.html

http://www.cisco.com/en/US/docs/net_mgmt/prime/network/3.10/user/guide/CiscoPrimeNetwork-UserGuide.html

http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/anyconnectadmin30.html

IEEE 802.1X/NAC Technology & Solution TOI, Mitsunori Sagae 2007

http://www.cisco.com/en/US/docs/security/ise/1.1/compatibility/ise_sdt.html#wp55038

http://support.microsoft.com/kb/929847

http://support.microsoft.com/kb/950725

http://support.microsoft.com/kb/309448/en-us

http://technet.microsoft.com/en-us/network/dd727529.aspx#EWKAC

http://windows.microsoft.com/en-sg/windows-vista/enable-802-1x-authentication

LIITTEET

Liite 1

Win XP SP3 PEAP-autentikaatio Microsoftin omalla supplikantilla LAN-verkossa

Liite 2

Win XP SP3 PEAP-autentikaatio Microsoftin omalla supplikantilla WLAN-verkossa

Liite 3

Win XP SP3 EAP-TLS-autentikaatio Microsoftin omalla supplikantilla LAN-verkossa

Liite 4

Win XP SP3 EAP-TLS-autentikaatio Microsoftin omalla supplikantilla WLAN-verkossa

Liite 5

Windows 7 PEAP-autentikaatio Microsoftin omalla supplikantilla LAN-verkossa

Liite 6

MAC Authentication Bypass toiminta testattavan verkkotulostimen osalta

ISE Network Device Authentication Summary

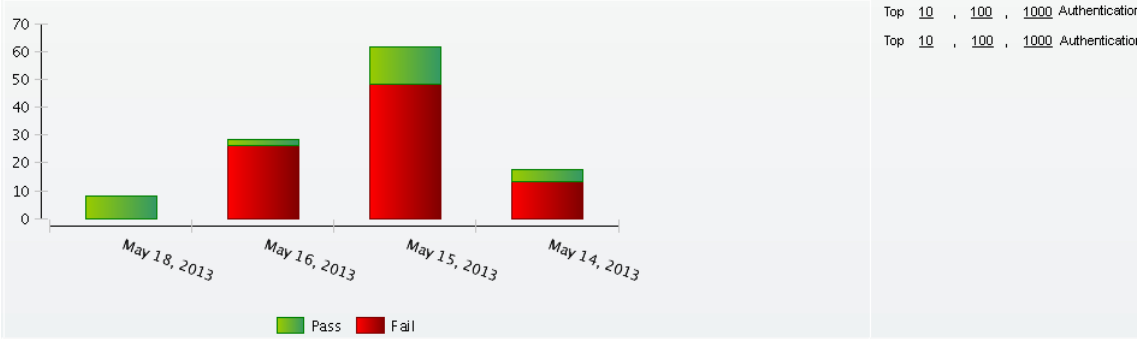
Network Device > Network Device Authentication Summary

Network Device : hml-tekniikka-tupala-95
Time Range : May 12,2013 - May 18,2013

Generated on May 19, 2013 3:56:07 PM EEST

27 Passed Authentication(s)
87 Failed Authentication(s)
114 Total

Authentications By Day and Quick Links



Day	Pass	Fail	Total	Fail %	Avg Response Time (ms)	Peak Response Time (ms)
May 18, 2013	8	0	8	0.00	39.12	86
May 16, 2013	2	26	28	92.86	10.46	117
May 15, 2013	13	48	61	78.69	13.34	98
May 14, 2013	4	13	17	76.47	16.18	61

Authentications By Failure Reason

Failure Reason	Total
22056 Subject not found in the applicable identity store(s)	83
12103 Failed to negotiate EAP because EAP-FAST not allowed in the Allowed Protocols	4

Authentications By Identity Group

Identity Group	Pass	Fail	Total	Fail %	Avg Response Time (ms)	Peak Response Time (ms)
	-	-	-	NaN		

Authentications By Network Device Group

Network Device Group	Pass	Fail	Total	Fail %	Avg Response Time (ms)	Peak Response Time (ms)
Device Type#All Device Types#LAN,Location#All Locations#Hml Ahvenisto	27	87	114	76.32	14.87	117

Authentications By Allowed Protocol

Allowed Protocol	Pass	Fail	Total	Fail %	Avg Response Time (ms)	Peak Response Time (ms)
Default Network Access	27	87	114	76.32	14.87	117

Authentications By Identity Store

Identity Store	Pass	Fail	Total	Fail %	Avg Response Time (ms)	Peak Response Time (ms)
AD1	25	0	25	0.00	34.84	86

Authentications By AD Domain

AD Domain	Pass	Fail	Total	Fail %	Avg Response Time (ms)	Peak Response Time (ms)
khshp.ad	25	0	25	0.00	34.84	86

Authentications By ISE Server

Server	Pass	Fail	Total	Fail %	Avg Response Time (ms)	Peak Response Time (ms)
khshpise	27	87	114	76.32	14.87	117